□ 信息安全系列丛书

基于身份的密码学

胡 亮 赵 阔 袁 巍
李宏图 初剑峰

The Cryptography Based on Identity

高等教育出版社
HIGHER EDUCATION PRESS

基于身份的密码学

本书介绍了基于身份密码研究的主要分支，包括：基于身份签名算法，基于身份加密算法，基于身份的分层加密与签名算法，基于无证书的签名及加密算法，第三方权力受约束的基于身份加密算法以及基于身份的广播加密算法等。

本书不仅包括一些典型的基于身份密码算法，同时也介绍了该领域国内外的最新进展。在内容的选择上，既突出广泛性，又注重对要点的深入探讨。语言简练，内容重点突出，逻辑性强，算法经典实用，使读者花少量的时间就能较快地掌握基于身份密码学的精髓。本书可作为密码学和信息安全专业的研究生或高年级本科生的教学参考书，也可作为密码学和信息安全领域的研究人员学习参考。

ISBN 978-7-04-031702-2
9 787040 317022 >
定价 39.00 元
学科类别：计算机
academic.hep.com.cn

□ 信息安全系列丛书

基于身份的密码学

胡 亮 赵 阔 袁 巍
李宏图 初剑峰

The Cryptography Based on Identity

JIYU SHENFEN DE MIMAXUE

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

基于身份的密码学/胡亮等著. —北京:高等教育出版社,2011.1

(信息安全系列丛书)

ISBN 978-7-04-031702-2

Ⅰ.①基… Ⅱ.①胡… Ⅲ.①密码-理论 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2011)第 003962 号

策划编辑 刘建元 **责任编辑** 刘建元 **封面设计** 王凌波

版式设计 余 杨 **责任校对** 姜国萍 **责任印制** 张福涛

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**咨询电话**	400-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
			http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京市白帆印务有限公司	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2011 年 1 月第 1 版
印 张	11.25	**印 次**	2011 年 1 月第 1 次印刷
字 数	210 000	**定 价**	39.00 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

物料号 31702-00

序

互联网、电子商务和电子政务的普及，在为社会经济发展带来巨大利益的同时，也带来了更加严峻的安全问题。在网络信息交互的应用环境中，除了信息加密等安全措施以外，还需解决信任问题。公钥基础设施（PKI，public key infrastructure）体系虽然从技术上可以解决网上认证、信息完整性和抗抵赖性等安全问题，但其安全保障是由证书来体现的，证书的管理和维护需要大量的处理资源和带宽资源，部署成本较高。

1984 年，以色列密码学家 Shamir 提出了基于身份的密码体系的思想，直接使用用户的标识，如姓名、电子邮件地址等作为公钥，而用户的私钥则通过一个被称作私钥生成器（PKG，private key generator）的可信任第三方进行计算得到。与传统的 PKI 体系相比，基于身份的密码学体系不再依赖证书，简化了管理密码体系的复杂性，成为密码学领域新兴的研究热点。

2001 年，第一个真正实用的基于身份加密（IBE，identity-based encryption）方案由美国密码学家 Boneh 和 Franklin 利用椭圆曲线上的双线性映射 Weil 配对设计出来。2002 年，美国密码学家 Gentry 和 Silverberg 第一次提出了一个完整建立在随机预言机模型下的、双线性 Diffie-Hellman 假设基础上分层的基于身份密码体系，从而解决了安全传输用户私钥的问题。2003 年，AI-Riyami 和 Paterson 提出了基于一个被称作密钥生产中心（KGC，key generator center）的可信第三方的无证书密码思想，以解决用户密钥由 PKG 托管的问题。2007 年，Goyal 提出了第三方权利受约束的基于身份加密方案（A-IBE，accountable authority identiy-based encryption scheme），在不改变 IBE 方案基础架构的前提下，进一步减少了用户对 PKG 的信任需求。

本书在介绍基于身份密码学研究分支的基础上，全面介绍了作者在基于身份签名算法、基于身份的广播加密算法以及基于身份的密码学典型应用实例方面所做的工作。全书九章安排如下：

第一章是基于身份密码学基础，主要介绍基于身份密码学的发展历程和本书使用的基础定义。

第二章是基于身份签名算法，主要介绍基于身份签名算法的构造模型，给出包括 Shamir 方案、CC-IBS 方案、Narayan 和 Parampalli 方案等在内的典型的基于身份签名方案，详细描述了作者提出的改进方案。

第三章是基于身份的加密算法，主要介绍基于身份加密算法的基础模型、Boneh 和 Franklin 的 IBE 方案、Waters 的 IBE 方案和 Gentry 的 IBE 方案，充分展现 IBE 系统的特点。

第四章是基于身份的分层加密算法（HIBE，hierarchical identity-based encryption），主要介绍相关的基本定义与 HIBE 安全模型、Gentry 和 Silverberg 方案、Boneh 等人的密文长度固定的 HIBE 方案、Au 等人的方案以及 Hu 和 Park 等人对 HIBE 和基于身份的分层签名算法（HIBS，hierarchical identity-based signature）的安全分析与改进。

第五章是基于无证书的签名算法，主要介绍相关的基础定义，以及安全模型、Riyami 的方案、Yum 和 Lee 的方案及分析、Zhang 等人的方案及安全性分析。

第六章是基于无证书的加密算法，主要介绍相关的安全模型、Riyami 的加密方案、Yum 和 Lee 的方案及分析、被动恶意 KGC 攻击、Au 等对 Riyami 方案的分析以及 Hwang 的模型。

第七章是 PKG 受约束的基于身份加密算法，主要介绍相关的定义和模型、Goyal 的 A-IBE 方案以及 Xu 等人的通用 A-IBE 方案。

第八章是基于身份的广播加密（IBBE，identity-based broadcast encryption）算法，主要介绍作者在相关的基本定义及基本模型、基于一次签名的构建方案、基于消息认证码（MAC，message authentication code）方式的构建方案以及基于 q-BDHI（q-bilinear Diffie-Hellman inversion problem）的 IBBE 方案等所做的工作。

第九章是基于身份密码应用，主要介绍作者设计并实现的密钥定时更换基础框架及其在防伪码系统和文件加密系统中的应用实例。

本书不仅包括一些典型的基于身份密码算法，同时也关注了该领域国内外的最新进展。在内容的选择上，本书既突出了广泛性，又注重对要点的深入探讨。语言简练，内容重点突出，逻辑性强，算法经典实用，便于读者花少量的时间尽快掌握基于身份密码学的精髓。

本书兼具专著和教材的双重属性，可作为密码学和信息安全专业的研究生或高年级本科生的教学参考书，也可供密码学和信息安全领域的研究人员学习参考。

作者

2010 年 12 月于长春

目　录

第一章　基于身份密码学基础

1.1　基于身份密码学概述

基于身份密码算法是一门新兴的且正在发展中的公钥密码算法，它的设计思想最早由以色列密码学家 Adi Shamir 提出。这种密码算法的设计目标是让通信双方在不需要交换公私密钥，不需要保存密钥目录，且不需要使用第三方提供认证服务的情况下，保证信息交换的安全性并可以验证相互之间的签名。

当前，影响公钥密码体制下安全系统发展的主要困难不是选择合适的安全算法或如何实施这些算法，而是部署和管理支持密钥真实性的基础设施。这些基础设施需要为用户提供公钥或用户身份与私钥之间关系的安全保证。在传统的公钥基础设施中（例如 PKI，public key infrastructure 体系），这种体系的安全保障是由证书来体现的，其本质是用权威机构来为用户签名。这种管理体制存在很多与证书管理相关的问题：包括撤销、存储和分配以及认证核查用户证书等。这需要占用大量的处理资源和带宽资源。

基于身份密码体制假设存在一个可信的私钥生成器（PKG，private key generator），当新用户第一次加入到网络中时，该中心会给每一个用户生成一个个性化的智能卡，卡中保存用户的私钥。用户可以使用私钥来对自己发送的信息进行加密和签名，同时还可以在不用考虑对方身份的情况下完全独立地解密并验证接收到的信息。

在传统的公钥基础设施中，智能卡在新的用户加入时往往不得不升级更新，而且各类认证中心需要协调其行为，保存一张所有用户的信息列表，并不断更新用户的信息，这使得认证中心的管理工作变得非常复杂。与其相比，基于身份的密码体系最大的优点是密钥生成中心可以在用户智能卡发行完成后关闭，网络可以在完全分散式的状态下运行任意的时间而不需要任何中心的支持。

在传统的公钥体系中，公钥的有效期在公钥证书生成时确定。如图 1.1，在基于身份加密算法中，一个实用系统的公钥终止前 Alice 可以使用公钥 Bob@jlu.edu.cn‖current year 来加密电子邮件，然后发送给 Bob，这样 Bob 只能使用他当年的私钥来实现解密。每年密钥到期后，Bob 需要从 PKG 中获取一个新的私钥，这样就达到了每年私钥到期更换的效果。与证书算法不同的是在每次 Bob

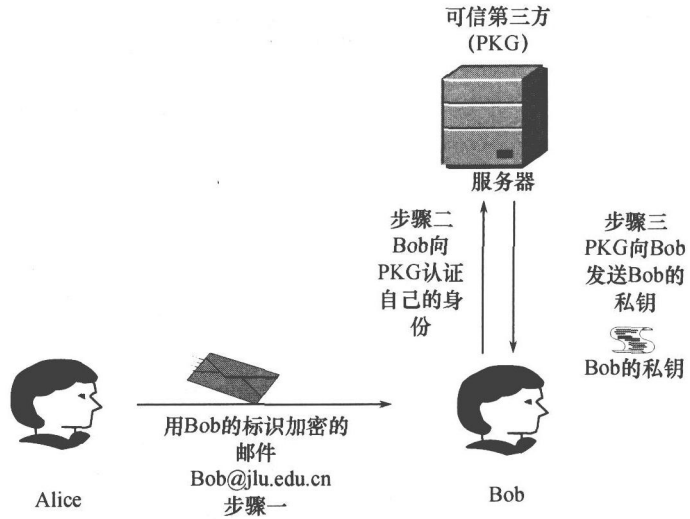

图 1.1 基于身份加密的执行过程

更新私钥后,Alice 并不需要获得新证书。一个更严谨的做法是使用"Bob@ jlu. edu. cn ‖current date"加密发送给 Bob 的电子邮件,这就迫使 Bob 每天需要获取新的私钥。因为 PKG 由公司自己管理,所以对于公司每天更新员工的私钥是可以做到的。有了这个方法,撤销密钥是非常简单的:Bob 离开公司时,他的主密钥需要撤销,公司的 PKG 停止向 Bob 的电子邮件地址发送私钥。因此,Bob 将无权阅读他的电子邮件,而且 Alice 不需要和任何第三方证书目录沟通来获得 Bob 的日常公钥。因此基于身份的加密对于实现需要经常更新的公钥机制是非常有效的。另外,Alice 还可以把信息发送到"未来",Bob 只能在由 Alice 规定的日期解密电子邮件。因为 PKG 可以很容易授予和撤销用户的密钥,通过这种方法,用户密钥的管理将变得非常简单。

在 Shamir 最初的设计中,这种密码算法特别适合于封闭的群体用户使用,例如跨国公司、大型银行的各个分支机构。因为这些公司的总部可以作为每一个用户所信任的密钥生成中心。基于身份的密码算法可以作为一种新的个人身份识别卡的基础,每一个用户可以用其进行电子签名验证、网上信用卡支付以及电子邮件的签名等活动。这种密码算法以传统公钥密码系统为基础,但也有一些不同之处:其中最核心的一点是公钥密码系统中随机生成公钥与私钥,并将其中的公钥公布。而这种算法使用用户自己选择的信息,如用户姓名、用户的电子邮件、电话号码等信息或这些信息的组合,作为其公钥使用,同时该用户也不能对代表自己的标识加以否定。与用户选择的公钥相对应的私钥则由密钥生成中心生成,并且在用户首次加入到该网络的时候以智能卡的形式颁发给该用户。

基于身份的密码算法就像一个完美的电子邮件系统;当知道对方的姓名和

地址,就可以给对方发送只能被对方读取的信息,同时可以验证来自于对方的签名。这样对于用户来说,通信的加密过程是透明的,所以它可以被对密钥和加密协议一无所知的非专业人员有效地使用。如:当用户 Alice 想给用户 Bob 发送信息时,Alice 使用自己智能卡中的私钥对信息进行签名,然后利用 Bob 用户的公钥对信息进行加密,把加密后的信息连同自己的身份信息发送给用户 Bob。当用户 Bob 收到信息后,首先使用自己的智能卡中的私钥对信息进行解密,然后使用 Alice 用户发来的身份信息验证 Alice 对信息的签名。

在这种密码算法中,用户的私钥不能由自己计算产生,必须由密钥生成中心计算产生。因为如果 Alice 能计算对应于公钥"Alice"的私钥,则同样也能计算出对应于"Bob"等公钥的私钥,这样就会对算法的安全性带来威胁。而密钥生成中心具有一定的特权,它可以知道一些特定的信息,利用这个信息可以为网络中的每一个用户计算出各自的私钥。这种算法的安全性依赖于以下几个因素:

(1) 基本加密算法的安全性;

(2) 密钥生成中心中特有信息的安全性;

(3) 在颁发给用户智能卡之前对用户身份标识核查的彻底性;

(4) 用户对智能卡丢失、被非法复制、非授权使用的防范性。

这种密码算法有效地将发送的信息与用户标识信息紧密联系起来,同时将用户的智能卡与用户本人也联系到一起。像其他发放身份识别卡的发卡机构一样,密钥生成中心应严格审查要发放智能卡的申请人,以避免非法用户冒称合法用户申请智能卡,同时密钥生成中心应保护好计算用户私钥所使用的特权信息以防止用户私钥泄露。对于一般用户而言,用户应该防止自己的智能卡遭到未经授权的使用,同时防止自己智能卡中的私钥在使用时被非法复制。

Shamir 指出,这种密码算法应当具有以下两个附加性质:

(1) 当已知种子密钥 k 后,可以容易计算出任意公钥对应的私钥;

(2) 如果已知任何一对公钥与私钥,计算出种子 k 是非常困难的。

同时,Shamir 也指出,由于 RSA(Rivest Shamir Adleman)加密方案不能同时满足这两个条件,因此不能应用到这种新算法中。因为如果模数 n 对于用户的标识符来说是一个伪随机过程,密钥中心不能将该模数 n 分解,也就不能从公钥 e 计算出私钥 d,假设模数 n 是一个具有一般意义的数,而种子是它的一个秘密的分解因子,这样任何一个知道公钥 e 和对应的私钥 d 的人都可以计算出种子。同时,Shamir 利用 RSA 算法构造了第一个基于身份的签名算法,并推断基于身份密码算法的实现是存在的,并将此问题作为一个公开问题提出,希望有人可以解决此问题。这与 1976 年 Diffie 和 Hellman 刚刚提出公钥密码学时的情况相似,虽然公钥密码学的设计思想被提出的同时也有了良好的应用前景,但是其具体的实现方案直到 1978 年才被研究出来。

自从 1984 年 Shamir 提出这个问题以来，很多基于身份的加密方案被陆续提出。然而，这些方案都不能完全令人满意。有些方案不能抵抗用户共谋，有些方案需要 PKG 对每个私钥请求花费很长的时间，有些方案则需要防硬件篡改。一个可用的基于身份的加密系统一直是一个重要但悬而未决的问题。直到 2001 年，第一个真正实用的基于身份加密（IBE，identity-based encrption）方案由美国密码学家 Boneh 和 Franklin 利用椭圆曲线上的双线性映射 Weil 配对设计出来。其中的公钥可以是任意字符串。该方案包含 4 个算法：

（1）*Setup* 生成全局系统参数和一个主密钥；

（2）*Extract* 使用主密钥生成对应于任意公钥字符串 $ID \in \{0,1\}^*$ 的私钥；

（3）*Encrypt* 使用公钥 *ID* 加密消息；

（4）*Decrypt* 使用相应的私钥解密消息。

该方案达到了 Shamir 提出的设计要求，即使接收者 Bob 尚未设置自己的公钥证书，发送者 Alice 也可以向他发送加密的邮件。该加密方案的性能与 ElGamal 算法性能相当，其安全性基于 Diffie-Hellman 假设。即只要计算双线性群 G_1, G_2 中的 CDH 问题（CDH，computaional Diffie-Hellman problem）是困难的。Boneh 和 Franklin 提出的 IBE 系统可以由 G_1, G_2 上的双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 构建，并在随机预言模型中达到选择密文安全。从此之后，这种体制的效率优势才开始被密码学界广泛关注。与传统的公钥密码学相比，基于身份的密码算法也有一些明显的缺点，如：每个用户从 PKG 的第三方接收自己的私钥，就需要用户向 PKG 认证自己作为合法接收者的身份，从而获取私钥，需要一个专门的安全信道向接收者传送私钥，这一过程存在一定的安全隐患和验证效率问题。为有效识别出一些恶意攻击者伪装成接收者申请私钥，提高验证效率以及私钥传输的安全性都是需要解决的问题，因此 PKG 必须公开嵌入用户私钥的参数信息。在 Alice 向 Bob 发送加密信息前，必须取得这些参数。由于 PKG 知道用户的私钥，也就是密钥托管是基于身份密码系统固有的。对于某些特定的应用，这种托管是一种优势，在一些大型的公司或需要谨慎分级管理事物的网络政务机构中是非常有效的。但对于另一些应用来说，这种托管是严重的安全问题。

不过，基于身份的加密技术的优势是引人注目的。与传统公钥密码学相比，获取真实公钥的问题已被获取公共 PKG 的真实参数问题取代，且后者负担较轻。因为相对总用户数来说，PKG 用户将有较大幅度的减少。一种极限情况是，如果每个人都使用一个 PKG，那么每个人都可以在系统中进行安全通信而不必在网上查询公钥或公共参数。虽然只有一个 PKG 的系统会完全消除网上参数的查询，但对一个大型网络来说，这样做是不可取的，因为这相当于把用户参数获取问题转化为 PKG 之间的参数传递问题。不仅生成私钥的计算代价高，而且必须对 PKG 进行身份验证并建立安全通道来传送私钥。

为了解决安全传输用户私钥的问题，2002 年美国密码学家 Gentry 和 Silverberg 在总结了前人研究成果的基础上第一次提出了一个完整建立在随机预言机模型下、双线性 Diffie-Hellman（BDH，bilinear Diffie-Hellman）假设基础上的分层基于身份密码算法（HIBC，hierarchical identity-based cryptography）该方案将 PKG 的功能分为多层，包括一个根 PKG 和多层的域 PKG。根 PKG 只为域 PKG 生成私钥，并对其进行身份认证。域 PKG 在得到私钥之后又可以利用自己的私钥为下层的域 PKG 生成私钥，直至最终用户的上一层，而这一层的 PKG 往往处于用户的本地或局域网中，这就使得对用户的认证和密钥的传输都在本地进行。如果低层 PKG 的密钥泄露，只会影响其域内用户，而不影响高层 PKG 私钥的安全性。

在基于身份密码算法中，用户私钥是由 PKG 利用主密钥产生的。同样 PKG 也能伪造任何实体的签名，因此这种算法不能提供真正的不可抵赖性。多 PKG 的提出和阈值技术的使用在一定程度上可以解决密钥托管问题，但是必须增加额外的通信和基础设施。因此，基于身份密码算法只能限于小范围或需要安全限制的应用。为了解决用户密钥由私钥生成中心托管的问题，AI-Riyami 和 Paterson 在 2003 年提出了无证书密码思想。在他们的方案中，同样需要一个被称作密钥生产中心（KGC，key generator center）的可信第三方。KGC 利用实体 A 的身份 ID_A 和主密钥为实体 A 提供部分私钥，并且这一过程是需要保密和认证的。也就是 KGC 必须保证这部分私钥必须安全地分发到正确的实体手中。

实体 A 将它的部分私钥和一些秘密信息结合生成实际的私钥 SA，因此 KGC 就不能获得 A 的私钥。实体 A 将它的一些秘密信息和 KGC 的公共参数结合计算出公钥 PA。由于 A 在生成 SA 时不需要 PA，公钥也不再仅仅从身份计算出来，所以这个系统不再是完全意义上的基于身份系统。实体 A 的公钥可以通过发送消息时添加附加信息或发布在公开的目录中以便其他用户使用。但是不需要额外的安全措施来保护 A 的公钥，特别是不需要证书。实体 B 只需要用 PA 和 ID_A 向 A 发送加密信息或验证 A 的签名。

由于缺少对公钥的认证信息（例如：公钥证书），所以敌手能够通过一个伪造的密钥来代替 A 的公钥。这似乎给敌手很大权力，并且也成为无证书公钥体制的一个漏洞。不过通过分析可知，敌手通过以上的攻击方式不能得到任何有价值的信息，因为计算正确的私钥需要由 KGC 生成的部分私钥，所以在没有正确的私钥的情况下，敌手不能解码被伪造的公钥加密的密文，也不能产生可以被伪造的公钥验证的签名等等。但必须假定 KGC 不能采用下面攻击的形式：因为可以获得实体的部分私钥，KGC 可以生成任何实体的公/私钥对并可以发布这个公钥，所以 KGC 可以扮演任何实体。也就是说，KGC 是被认为不会替换实体公钥的。但是 KGC 可以从事其他的敌对活动，例如：对密文进行窃听，并解密密

文。在基于身份密码算法中,用户必须信任 PKG 不会去滥用私钥;但在无证书密码中,用户仅仅需要相信 KGC 不去发布伪造的公钥。与基于身份密码算法相比,无证书密码中对可信任第三方的信任依赖可以大幅降低。

由于 PKG 有能力计算任何身份所对应的私钥,基于无证书机制虽然降低了对 PKG 的信任度,但并未完全解决这一问题。实际上,只要需要信任 PKG,当 PKG 滥用其权利时,完全信任和部分信任使得基于身份的密码系统都存在安全缺陷。也就是说,如果 PKG 愿意,它可以自由地从事任何的恶意行为却不会面临任何法律制裁。这些恶意行为可能包括:为任何的用户解密和读取信息,或者更糟的是,可以为任何身份生成和分配私钥。尽管它具有很出色的性能,但事实上已经成为减缓 IBE 使用的一个重要原因。由于存在密钥托管或部分密钥托管问题,IBE 的用户被限制在小的且封闭的组中,该组中只有一个中心受信权威是可用的,这些都引起了对该体系的广泛争论。

2007 年,Goyal 创造性地提出了一种对密钥托管问题的完全解决方案。该方案在不改变 IBE 方案基础结构的条件下,进一步减少了用户对 PKG 的信任需求。该方案称为第三方权利受约束的基于身份加密方案(A-IBE, accountable authority identity-based encryption scheme)。

总的来说,在 A-IBE 方案的密钥生成协议中,当用户收到来自 PKG 的私钥种子信息时,用户通过秘密选取“迹”信息来部分地决定用户私钥的生成。因此,从直觉上来说,由于 PKG 并不知道用户秘密选取的“迹”,因此也就无法独立生成具有相同“迹”的该用户的私钥。另一方面,由于私钥种子信息的秘密性,用户在没有 PKG 的帮助下也无法额外地生成不同“迹”的私钥。因此在实际应用中,若某用户发现有人知道他的一个有效的且不同“迹”的私钥时,那么该用户就可以充分地认定 PKG 伪造了他的私钥,从而进行索赔。较具体地说,Goyal 首次给出了 A-IBE 的定义及其特殊的安全性定义,并且分别基于 Gentry 和 Waters 的 IBE 方案,构造了两个具体的可证明安全的 A-IBE 方案。Goyal 方案的特点如下:

(1) 在这个 IBE 方案中,对应每个身份 ID 都可能存在指数个解密密钥。

(2) 已知一个身份的解密密钥,想获得其他的解密密钥是很困难的。

(3) 用户们使用一个安全密钥产生协议,从 PKG 上面获取与其自身身份所对应的解密密钥。这个协议允许用户为其身份获得一个单独的解密密钥 d_{ID},而不需要让 PKG 知道具体获得了哪一个。

(4) 如果 PKG 为有恶意用途的身份产生一个解密密钥 d'_{ID},尽管这种可能微乎其微,但是它也将区别于用户所获得的密钥 d_{ID}。因此密钥对(d'_{ID},d_{ID})将会成为 PKG 恶意行为的证据(因为在正常情况下,每个身份只能有一个密钥)。

虽然 PKG 确实能够被动地解密所有用户信息。但是,对于私钥 d'_{ID}的分配

来说 PKG 是被严格限制的。密钥 d'_{ID} 的完整信息使实体 E 与诚实用户 U(具有身份 ID 和密钥 d_{ID})能够一起合作,将(d'_{ID},d_{ID})作为欺诈证据对 PKG 提出控告(进而可能停止它的业务或给 E 和 U 大量金钱作为补偿,这将是 E 和 U 乐于接受的)。这意味着在任何时候,如果 PKG 为有恶意目的身份产生解密密钥的话,那么将存在陷入高额索赔的风险。

在基于身份密码学的基础上,研究基于身份的广播加密算法也具有重要的应用价值。广播加密(BE,broadcast encryption)是由 Fiat 和 Naor 提出的。一个广播者加密消息给监听广播信道的一组用户 S。在集合 S 中的用户可以用自己的私钥解密广播的消息。

Delerablée、Paillier 和 Pointcheval 扩展了广播加密的概念,提出了动态广播加密(DBE,dynamic broadcast encryption)。一个动态广播加密系统是一个开始并不把所有用户都初始化的广播加密系统。基于此特性,任意新用户都可以对之前分发的密文进行解密。因此,动态广播加密系统适合于很多应用,比如 DVD 加解密。然而,许多应用例如 VOD 视频点播,需要前向安全,这时动态广播加密系统就不适合了。最初,Delerablée 使用了略强的攻击模型,该攻击模型允许挑战者在获得系统公开参数之前适应性地选择密文,这是静态攻击模型的一个增强版。

Smart 提出的多接收者密钥封装机制(mKEM, multi-receiver key encapsulation)是一个有效的多步的密钥封装机制。后来,mKEM 的概念被扩展为多个基于身份接收者的密钥封装机制(mID-KEM,multi-receiver identity-based key encapsulation),密文的长度随着接收者的数目而增长。Chatterjee 和 Sarkar 提出了第一个 mID-KEM 协议来达到子线性的密文长度,密文的长度是 $|S|/N$,其中私钥的长度是 N,S 是接收者身份集合。因此,他们介绍了第一个 Mid-KEM 协议,实现了子线性的密文个数。最近,Abdalla 等提出了一种方案,采用不变大小的密文,但是私钥的数量是 $o(n^2_{\max})$。

在总结以上方案的基础上,本书分别利用一次签名机制和 MAC 机制构造了两个高效的基于身份广播加密算法。

1.2 基础定义

1.2.1 双线性映射

定义 1 双线性映射(指数形式)。设 G_1 是由 g 产生的循环加法群,它的阶是素数 p,G_2 是同阶的循环乘法群,映射 $e:G_1\times G_1\rightarrow G_2$ 是一个线性映射,如果映射满足下面的条件:

(1) 双线性:对于所有的 $u,v\in G,a,b\in Z_p$,有 $e(u^a,v^b)=e(u,v)^{ab}$。

(2) 非退化性:存在 $e(g,g)\neq 1$。

(3) 可计算性:对于所有的 u,v,存在一个有效的算法计算 $e(u,v)$。

定义 2 双线性映射(对数形式):我们称映射 e 是双线性映射,如果:G_1 是一个 q 阶加法循环群,G_2 是一个 q 阶乘法循环群,$G_1\times G_1\rightarrow G_2$ 具有以下属性:

(1) 双线性:对任意 $Q,R\in G_1,a,b\in Z$,有 $e(aQ,bR)=e(Q,R)^{ab}$。

(2) 非退化性:该映射不把 $G_1\times G_1$ 上的所有配对映射到 G_2 上。

(3) 可计算性:存在一个有效的算法对于任何 $Q,R\in G_1$,可以计算 $e(Q,R)$。

1.2.2 数学难题与安全性

各种数学难题和假设是构建密码学安全性的基础,而安全性的高低直接决定了一个密码学方案的安全强度。本节在对典型的数学难题进行回顾的基础上,进一步总结了 IBE 方案安全性的各种数学难题基础。

DH 相关问题(DHP,Diffie-Hellman problem)

DH 问题:

定义 3 给定一个大素数 q,一个大整数生成元 $g\in Z_q^*$,以及由大随机数 a,b 生成的 $g^a \bmod q$ 和 $g^b \bmod q$,要求找到 $g^{ab} \bmod q$。

DH 问题是 Diffie-Hellman 密钥交换算法安全性的基础,这种安全性是建立在有限域内计算离散对数(DL,discrete logarithm)的困难性基础之上的。

CDH 问题(CDH,computational Diffie-Hellman problem):

定义 4 对于随机给定的$\langle P,aP,bP\rangle$,其中 a,b 属于具有 q 阶的点群 Z_q^*,计算 abP 的值。

同 DH 问题一样,CDH 问题的困难性也是基于离散对数的。

DDH 问题(DDH,decision Diffie-Hellman problem):

定义 5 区分对于给定的元组$\langle P,aP,bP,abP\rangle$和$\langle P,aP,bP,cP\rangle$之间的分布,即判断 c 是否等于 $ab \bmod q$,其中 a,b,c 属于具有 q 阶的点群 Z_q^*。

在具有 q 阶的加法循环点群 G_1 上,DDH 问题的判定是容易的。因为在群 G_1 上,对于给定的 $P,aP,bP,cP\in G_1$,可以构造出多项式时间可计算的双线性映射 e,来验证 $c=ab \bmod q\Leftrightarrow e(aP,bP)=e(P,cP)$。

q-DHI 问题(q-DHI,q-Diffie-Hellman inversion problem):

定义 6 给定 $q+1$ 维元组$\langle g,g^x,g^{x^2},\cdots,g^{x^q}\rangle\in G^{q+1}$,计算 $g^{1/x}\in G$。

q-DHI 假设为一个更自然的复杂性假设,且问题描述中不要求使用随机预言机模型。因此,基于 DH 假设的构建可以被依赖于 q-DHI 假设的构建所取代。

q-SDH 问题(q-SDH,q-strong Diffie-Hellman inversion problem):

定义 7 给定维 $q+1$ 元组$\langle g,g^x,g^{x^2},\cdots,g^{x^q}\rangle\in G$,计算$(c,g^{1/(x+c)})$,其中 c,

$x \in Z_q^*$。

当 c 固定时，SDH 问题等价于 DHI 问题。

BDH 问题(BDH, bilinear Diffie-Hellman problem)：

定义 8 设 G_1 和 G_2 为两个具有素数 q 阶的点群，$e: G_1 \times G_1 \to G_2$ 为一个可采纳的双线性映射，P 为 G_1 的生成元，对于给定的$\langle P, aP, bP, cP\rangle$，其中 $a, b, c \in Z_q^*$，计算 $W = e(P,P)^{abc} \in G_2$。

通过分析发现，$\langle G_1, G_2, \hat{e}\rangle$中的 BDH 问题并不比 G_1 或 G_2 上的 CDH 问题更难，也即 G_1 或 G_2 上的一个 CDH 算法足以解决$\langle G_1, G_2, e\rangle$中的 BDH 问题。

q-LBDH 问题(q-LBDH, q-list bilinear Diffie-Hellman problem)：

定义 9 给定元组$\langle g, g^a, g^b, g^c\rangle \in (G_1)^4$，其中 $a, b, c \in Z_q^*$，输出一个长度最大为 $q(q \geqslant 1)$的列表 L，且 L 中包含 $e(g,g)^{abc} \in G_2$。

DBDH 问题(DBDH, decision bilinear Diffie-Hellman problem)：

定义 10 区分给定元组$\langle g, g^a, g^b, g^c, e(g,g)^{abc}\rangle$和$\langle g, g^a, g^b, g^c, e(g,g)^z\rangle$的分布，即判断 z 是否等于 $abc \pmod q$，其中 a, b, c 属于具有 q 阶的点群 Z_q^*。

GBDH 问题(GBDH, gap bilinear Diffie-Hellman problem)：

定义 11 给定元组$\langle g, g^a, g^b, g^c\rangle \in (G_1)^4$，在 DBDH 预言机 O(对于给定的$\langle g, g^a, g^b, g^c, T\rangle \in (G_1)^4 \times G_2$，如果 $T = e(g,g)^{abc}$，则为 ture，否则为 false)的帮助下，输出 $e(g,g)^{abc} \in G_2$。

q-BDHE 问题(q-BDHE, bilinear Diffie-Hellman exponent problem)：

定义 12 给定$\langle h, g, g^x, g^{x^2}, \cdots, g^{x^q}, g^{x^{q+2}}, \cdots, g^{x^{2q}}\rangle \in G_1^{2q+1}$，其中 $x \in Z_q^*$，计算 $e(g,h)^{(x^{q+1})} \in G_2$。

q-ABDHE 问题(q-ABDHE, q-augmented bilinear Diffie-Hellman exponent problem)：

定义 13 给定$\langle g', g'^{(x^{q+2})}, g, g^x, g^{x^2}, \cdots, g^{x^q}, g^{x^{q+2}}, \cdots, g^{x^{2q}}\rangle \in G_1^{2q+2}$，其中 $x \in Z_q^*$，计算 $e(g,g')^{(x^{q+1})} \in G_2$。

定义 14 截断判定性 q-ABDHE 问题(q-ABDHE, truncated decision q-augmented bilinear Diffie-Hellman exponent problem)。

已知一个有 $q+3$ 个元素的矢量

$$(g', g'^{(\alpha)^{q+2}}, g, g^\alpha, g^{(\alpha)^2}, \cdots, g^{(\alpha)^q}) \in G_1^{q+3}$$

元素 $Z \in G_2$ 作为输入，如果 $Z = e(g^{(\alpha)^{q+1}}, g')$，输出 0，否则输出 1。

如果

$$\left| Pr[B(g', g'^{(\alpha)^{q+2}}, g, g^\alpha, \cdots, g^{(\alpha)^q}, e(g^{(\alpha)^{q+2}}, g')) = 0] - Pr[B(g', g'^{(\alpha)^{q+2}}, g, g^\alpha, \cdots, g^{(\alpha)^q}, Z)] \geqslant \varepsilon \right|$$

就说算法 B 以 ε 的优势解决了截断判定性 q-ABDHE 问题。

其中的概率指的是生成元 g,g' 在 G_1 内随机选取，α 在 Z_p 内随机选取，Z 在 G_2 中随机选取，以及 B 使用的随机位。式子的左边是 P_{ABDHE}，右边是 R_{ABDHE}。

q-BDHI 问题（q-BDHI，q-bilinear Diffie-Hellman inversion problem）：

定义 15　给定 $q+1$ 维元组 $\langle g,g^x,g^{x^2},\cdots,g^{x^q}\rangle \in (G_1^*)^{q+1}$，其中 $x \in Z_q^*$，计算 $e(g,g)^{1/x} \in G_2$。

显然，当 $q=1$ 时，1-BDHI 假设等同于标准的 BDH 假设。

q-DBDHI 问题（q-DBDHI，q-decision bilinear Diffie-Hellman inversion problem）：

定义 16　给定 $\langle g,g^x,g^{x^2},\cdots,g^{x^q},k\rangle$，其中 $x \in Z_q^*$，$g \in G_1$，$k \in G_2$，判断 k 是否等于 $e(g,g)^{1/x}$，若等于，输出“是”；否则，输出“否”。

q-ABDHI 问题（q-ABDHI，q-augmented bilinear Diffie-Hellman inversion problem）：

定义 17　给定 $\langle g^{(x^{q+2})},g,g^x,g^{x^2},\cdots,g^{x^q}\rangle \in G_1^{q+1}$，其中 $x \in Z_q^*$，计算 $e(g,g)^{1/x} \in G_2$。

q-wBDHI 和 q-wBDHI* 问题（q-wBDHI，q-weak bilinear Diffie-Hellman inversion problem）：

定义 18　q-wBDHI：给定元组 $\langle g,h,g^x,g^{x^2},\cdots,g^{x^q}\rangle$，其中 $g,h \in G_1$，$x \in Z_q^*$，计算 $e(g,h)^{1/x}$。

定义 19　q-wBDHI*：给定元组 $\langle g,h,g^x,g^{x^2},\cdots,g^{x^q}\rangle$，其中 $g,h \in G_1$，$x \in Z_q^*$，计算 $e(g,h)^{(x^{q+1})}$。

图 1.2 展示了一些数学难题之间的强弱关系，其中单向箭头所指方向表示数学难题的难度增强，双向箭头两侧的数学难题是等价的。

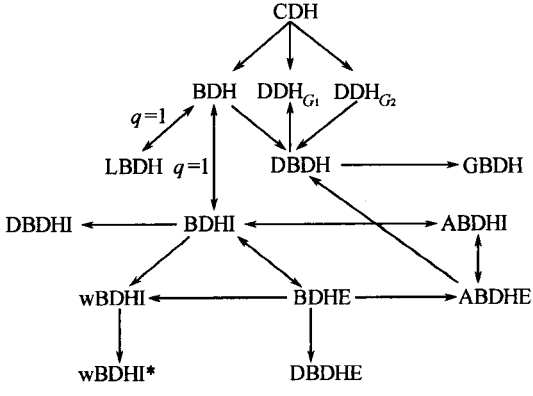

图 1.2　各种数学难题之间的强弱关系

从图 1.2 中的描述可以得出，加法点群 G_1 上的 CDH 问题要难于 DDH 问

题,因为可以通过可计算的双线性映射 e,来验证 $c = ab(\mathrm{mod}\, q) \Leftrightarrow e(aP, bP) = e(P, cP)$。$G_1$ 或 G_2 中的 CDH 问题足以解决$\langle G_1, G_2, e\rangle$中的 BDH 问题,但是反过来,一个 BDH 问题是否足以解决 G_1 或 G_2 中的 CDH 问题仍然是一个开放性问题,有待于进一步的证明。在 $q = 1$ 时,BDHI 问题和 LBDH 问题都等价于 BDH 问题,而当 $q > 1$ 时,并不能确定 BDH 和 BDHI 问题是否等价。q-BDHI 问题是$(q+1)$-BDHE 问题的一个特例,难度是相似的,不同之处在于$(q+1)$-BDHE 问题给出了更多 G_1 上的额外值,但是这些额外值对于问题的解决并没有提供任何帮助。q-ABDHI 和 q-ABDHE 是对 q-BDHI 和 q-BDHE 在参数上的扩展,它们之间是等价的,可以通过$(g', g'^{(x^{q+2})}) = ((g^{(x^{-q-2})})^x, g^x)$进行转换。$q$-ABDHE 的判定问题要强于 DBDH 问题,$q$-ABDHI 问题等价于 q-BDHI 问题。wBDHI 问题和 wBDHI* 问题在线性时间约简下是等价的,且在任何相同的点群下,他们的安全性假设弱于 BDHI 和 BDHE 问题。此外,图中还展示了一个一般规律,即数学难题的难易程度与生成元所在的点群类型和大小相关。在相同点群下通常计算问题要难于判定问题;而在不同点群下,数学难题的难易程度往往不易比较。但通常点群越大,数学难题就越难,由此所带来的安全性也就越高。

参考文献

[1] Shamir A. Identity-based cryptosystems and signature schemes, LNCS, 1985, Vol. 196:47-53.

[2] Boneh D, Franklin M. Identity based encryption from the Weil pairing, Lecture notes in computer science,2001, Vol. 2139: 213-229.

[3] Al-Riyami S S, Paterson K G. Certificateless public key cryptography, LNCS,2003, Vol. 2894: 452-473.

[4] Delerablée C. Paillier P,Pointcheval D. Fully collusion secure dynamic broadcast encryption with constant-Size ciphertexts or decryption keys, LNCS,2007, Vol.4575: 39-59.

[5] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups, Lecture notes in computer science,2003, Vol. 2567: 18-30.

[6] Yi X. An identity-based signature scheme from the Weil pairing, Communications letters, 2003, Vol. 7: 76-78.

[7] Yuen T H, Susilo W, Mu Y. How to construct identity-based signatures without the key escrow problem, International journal of information security, 2010, Vol. 9, No. 4: 297-311.

[8] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model, Lecture notes in computer science,2006, Vol. 4058: 207-222.

[9] Gentry C. Practical identity-based encryption without random oracles, Lecture notes in

computer science,2006, Vol. 4404: 445-464.

[10] Boneh D, Boyen X. Efficient selective-ID identity based encryption without random oracles, Lecture notes in computer science,2004, Vol. 3027: 223-238.

[11] Gentry C. Practical identity-based encryption without random oracles, Lecture notes in computer science,2006, Vol. 4404: 445-464.

[12] Waters B. Efficient identity-based encryption without random oracles, Lecture notes in computer science,2005, Vol. 3494: 114-127.

[13] Boneh D, Franklin M. Identity-based encryption from the Weil pairing, Lecture notes in computer science,2001, Vol. 2139:213-29.

[14] Gentry C, Silverberg A. Hierarchical ID-based cryptography, Lecture notes in computer science,2002, Vol. 2501: 548-566.

[15] Boneh D, Boyen X, Goh E -J. Hierarchical identity based encryption with constant size ciphertext, Lecture notes in computer science,2005, Vol. 3494: 440-456.

[16] Goyal V. Reducing trust in the PKG in identity-based cryptosystems. In: Advances in Cryptology-Crypto 2007, LNCS,2007, vol. 4622: 430-447.

[17] Xu P, Cui G H, Fu C, et al. A more efficient accountable authority IBE scheme under the DL assumption. Sci China Inf Sci,2010, 53: 581-592.

[18] Smart N P. Efficient key encapsulation to multiple parties, LNCS,2004, 3352:208-219.

[19] 胡亮,刘哲理,孙涛,刘芳. 基于身份密码学的安全性研究综述. 计算机研究与发展, 2009.9, Vol.46 No.9:1537-1548.

[20] Zhang M, Zhang Y, Hu L. A faster algorithm for matching a set of patterns with variable length don't cares. Information processing letters, Feb, 2010, Vol.110, No.6:216-220.

[21] Hu L, Liu Z, Cheng X. Efficient identity-based broadcast encryption without random oracles. Journal of Computers, Mar, 2010, Vol.5, No.3: 331-336.

第二章　基于身份签名算法

2.1　基于身份签名算法介绍

基于身份密码体制(IBC,identity-based cryptosystem)概念的提出可以追溯到1984年Shamir对此的开创性工作。随后,一些应用大整数因数分解问题的基于身份的加密和签名方案被提出。2000年Sakai与Boneh-Franklin独立提出了以双线性对为基础的基于身份的加密体制后,基于身份密码体制的研究领域得到了重新的关注。2001年以后,更多的基于双线性映射的方案被提出,其中亦包括基于身份的签名方案(IBS,identity-based signature scheme)。

2000年,Sakai就提出了一种基于身份的签名方案,但是在那篇文章中,Sakai并没有给出相关的安全性分析。2002年,Paterson独立提出了一种在椭圆曲线配对下的基于身份的签名方案,虽然Paterson对其方案进行了分析,但同样没有给出完整的安全性证明。直到2003年,Cha和Cheon在Boneh-Franklin的加密方案基础上,给出了完整的基于身份签名方案和该方案在随机预言模型(ROM,random oracle model)下的安全性证明。

大多数基于身份的签名方案都是在随机预言模型下被证明是安全的。这些方案以存在一个随机过程为基础(或者说Hash函数被认为是一个随机预言)。在随机预言模型方案中存在的对签名不可伪造性攻击都是利用攻击随机预言的返回值(也称哈希值)来完成的。不过,同样存在利用构造抗碰撞的Hash函数来进行随机预言模型下对签名的密码学攻击的方案。虽然随机预言的方法是可行的,但是其安全性是建立在敌手对随机预言查询预测能力有限的前提下。随着敌手计算机性能的不断发展,有必要建立在实际应用中不受敌手计算性能限制的模型。标准模型安全框架可以更好地模拟实际应用情况。

2004年以后,在标准模型下的证明技术重新得到了关注。在证明的安全性的过程中,期望不依靠随机函数生成随机值的安全性来保证体制的安全,而是让敌手去攻击模型中潜在的数学难题来保证模型的安全性。解决这种问题是一项困难的任务,不同于随机预言模型,在标准模型中敌手执行的计算过程不是在解决一个其他的实体函数值(Hash函数值)的预测问题,而是在解决一个潜在的数学难题。

在标准模型下第一个直接构造出高效的基于身份签名方案的人是 Paterson 和 Schuldt,他们使用了由 Gentry 和 Silverberg 提出的两级分层的基于身份的加密算法来实现基于身份的签名方案。该方案中包含了由 Waters 在标准模型下构建的第一个高效的基于身份的加密方案中的 Waters-Hash 方法。Paterson 和 Schuldt 将 Waters-IBE 按层次扩展构建了他们的方案。该方案在计算上具有较高的效率,同时它使用计算 Diffe-Hellman 难题作为其安全性的基础。

2008 年,Hu 和 Li 针对 Paterson 和 Schuldt 的方案,提出了一种简化的基于身份签名方案。同年 Narayan 和 Parampalli 提出了在标准模型下的基于身份的签名方案,即标准签名(SS,standard signature)方案,与 Paterson 和 Schuldt 的方案相比,对公共参数进行了简化。Narayan 和 Parampalli 在方案中提出了一些额外的属性。数字签名可以按照验证的范围的大小分为两类:第一类是指签名具有传递性,每一个人都可以验证被签名消息的真伪。第二类数字签名不具有传递性,不能被公共域内的人验证,只有消息的接收者才能验证其签名。数字签名通常应该具有公用的验证性,但是在特殊的通信场景中交流的信息为用户私有的情况下,我们希望它不具有这种公共验证性。在基于身份条件的签名方案中,可以利用关联接收者的身份来验证签名的方法来使其验证具有非传递性。在这种约束条件下,任何第三方在缺少接收者身份时不能验证签名的真伪。

2.2 基于身份签名的构造模型

2.2.1 基于身份签名的定义

基于身份签名方案是一组安全参数为 k 的多项式时间算法 $IBS = (Setup, KeyDer, Sign, Vf)$ 组成的。

Setup:输入 k 比特的安全参数,输出主公/私钥对(mpk, msk)。

KeyDer:输入 msk 和 id,生成身份为 $id \in \{0,1\}^*$ 的用户私钥 usk,并将 usk 安全地发送给该用户。

Sign:输入 usk 和消息 m,返回对消息 m 的签名 σ。

Vf:输入 mpk, id, m 和 σ,如果 σ 对于 id 和 m 是有效的,则返回 1;否则,返回 0。

方案不可伪造性的安全性证明是在选择消息和选择身份攻击下,通过一个伪造者 $\mathcal{F}$和一个参数化的安全性参数 k 的实验来定义的。这个实验以新的主密钥对$(mpk, msk) \leftarrow Setup(k)$的产生开始,伪造者 $\mathcal{F}$使用输入的主公钥 mpk 来运行,并能访问以下预言:

KeyDer(·):输入 msk 和身份 $id \in \{0,1\}^*$,返回一个秘密签名密钥 $usk \leftarrow$

$KeyDer(msk,id)$。

$Sign(\cdot,\cdot)$:输入密钥 usk 和消息 $m\in\{0,1\}^*$,返回一个签名 $\sigma\leftarrow Sign(usk,m)$,其中 $usk\leftarrow KeyDer(msk,id)$。

结束时,伪造者输出身份 id^*、消息 m^* 和伪造的签名 σ^*。如果 $Vf(mpk,id^*,m^*,\sigma^*)=1$ 而且 $\mathcal{F}$ 从未问询过 $KeyDer(\cdot,id^*)$ 和 $Sign(\cdot,m^*)$,那么就说伪造者 $\mathcal{F}$ 赢得了游戏。用优势 $Adv^{uf\text{-}cma}_{IBS,\mathcal{F}}(k)$ 来定义 $\mathcal{F}$ 赢得游戏的概率,而且如果对于所有多项式时间的伪造者 $\mathcal{F}$, $Adv^{uf\text{-}cma}_{IBS,\mathcal{F}}(k)$ 都是可以忽略的,就说 IBS 能抵制选择消息攻击下的不可伪造性(uf-cma)。

2.2.2 标准签名方案到基于身份签名的转换(*SS-2-IBS* 转换)

标准签名方案是由三个多项式时间算法 $SS=(KeyGen,Sign,Vf)$ 组成的。算法 $KeyGen$ 以安全参数 k 作为输入,产生一个密钥对 (pk,sk)。签名者通过 $\sigma\leftarrow Sign(sk,m)$ 创建消息 m 的签名,然后验证者通过测试 $Vf(pk,m,\sigma)=1$ 的真假来检查签名的有效性。

安全性是通过选择消息攻击的不可伪造性(uf-cma)来证明的。具体描述如下:伪造者 $\mathcal{F}$ 输入一个新的公钥 pk,并被给予对应私钥 sk 的签名预言的访问权限。如果伪造者能够输出一对 (m^*,σ^*) 使得 $Vf(pk,m^*,\sigma^*)=1$ 而且没有对 m^* 进行过签名预言问询,那么伪造者就成功伪造签名。

用优势 $Adv^{uf\text{-}cma}_{SS,\mathcal{F}}(k)$ 来定义 $\mathcal{F}$ 成功的概率。如果对所有的多项式时间伪造者 $\mathcal{F}$ 在 k 取值范围内优势 $Adv^{uf-cma}_{SS,\mathcal{F}}(k)$ 都是可以忽略的,那么就说 SS 是 uf-cma 安全的。

给定一个标准签名方案 $SS=(KeyGen,Sign,Vf)$,可以按如下的方法建立一个基于证书的 IBS 方案 $Cert\text{-}IBS=(Setup,KeyDer,Sign',Vf')$。并且很容易证明,如果 SS 是 uf-cma 安全的,那么 $Cert\text{-}IBS$ 也是 uf-cma 安全的。如下页图 2.1 所示。

2.2.3 规范鉴别方案到基于身份签名的转换(*cSI-2-IBS* 转换)

一个标准身份鉴别(SI, standard identification)方案由三个多项式时间算法 $SI=(KeyGen,P,V)$ 组成。算法 $KeyGen$ 以安全参数 1^k 作为输入,输出一个新的密钥对 (pk,sk)。证明和验证算法 P 和 V 的交换形成了身份鉴别协议。算法 P 以密钥 sk 作为输入,与以公钥 pk 为输入的算法 V 进行交互。V 输出 0 或者 1 来表示算法 P 是否被成功地鉴别。

方案 2.1 *IBS = Cert-IBS*

Setup(k):
  (mpk,msk)←*KeyGen*(1^k)
  return (mpk,msk).
KeyDer(msk,id):
  (pk,sk)←*KeyGen*(k);$cert$←*Sign*(msk,$pk \parallel id$)
  return usk←(sk,pk,$cert$).
Sign'(usk,m):
  Parse usk as (sk,pk,$cert$);σ←*Sign*(sk,m)
  return σ'←(σ,pk,$cert$).
Vf'(mpk,id,m,σ'):
  Parse σ' as(σ,pk,$cert$)
  If *Vf*(pk,m,σ) = 1 and *Vf*(mpk,$pk \parallel id$,$cert$) = 1 then d←0 else d←1
  return d.

图 2.1 *SS-IBE* 转换

安全性通过在被冒充攻击(imp-pa)下的抵抗性来证明。具体描述如下:敌手 $\mathcal{A}$(冒充者)获得一个新的公钥 pk,并有权查询 $P(sk)$ 和 $V(pk)$ 算法之间的交互返回值的预言(要想方案是安全的,协议就必须是随机化的,所以每一次请求的返回都是不同的并且是随机的)。如果 $V(pk)$ 最后输出 1,冒充者 $\mathcal{A}$ 就赢得游戏。$\mathcal{A}$ 赢得游戏的概率用优势 $Adv_{SI,\mathcal{A}}^{imp\text{-}ma}(k)$ 来表示,如果 $\mathcal{A}$ 的优势是可以忽略的,那么就说 *SI* 是 imp-pa 安全的。在定义 SI 方案的转换方法之前,我们需要介绍陷门-取样(trapdoor-samplable)的关系。

定义 陷门-取样关系族 F 是三元多项式时间算法(TDG,Smp,Inv),具有如下的性质:

可计算性:输入安全参数 k,TDG 输出具有陷门信息 t 的关系:$R \subseteq Dom \times Rng$ 其中 $Dom = R(x) = \{y \mid (x,y) \in R\}$,$Rng = R^{-1}(y) = \{x \mid (x,y) \in R\}$。

可采样性:算法 Smp,输入关系 R,输出从 R 产生的随机二元组。

可逆性:输入关系 R,对应的陷门信息 t,和一个元素 $y \in Rng$,算法 Inv 随机输出 $R^{-1}(y)$ 中的一个元素。

正则性:对 F 中的每个关系 R,都有一个整数 d 使得对于所有的 $y \in Rng$,都有 $|R^{-1}(y)| = d$。

若一个 SI 方案 $SI = (KeyGen, P, V)$ 的密钥产生过程依赖一个陷门-取样关系族,就说方案 SI 是可转换的身份鉴别方案(cSI)。注:必须存在一个族 $F = (TDG, Smp, Inv)$ 使得由 $KeyGen$ 产生的密钥满足 $pk = (R,y)$ 和 $sk = (R,x)$ 并依据下面的关系分布:

$$(R,t) \leftarrow TDG(1^k); (x,y) \leftarrow Smp(R)$$

一个 cSI 方案 $SI = (KeyGen, P, V)$ 是规范的,符合以下:

(1) P 随机从承诺集合($CmtSet(R)$)中选取某个"承诺" cmt 来初始化通信,

其中集合 $CmtSet(R)$ 是依赖嵌入于公钥和私钥的关系产生的。

(2) V 从挑战集合($ChSet(R)$)随机地选择某个"挑战"ch 并返回。

(3) P 用"回应"rsp 来应答;然后 V 根据公钥和通信副本对做出决策函数 $dec(pk, cmt \| ch \| rsp) \in \{0,1\}$。其中 $1/|CmtSet(R)|$ 是可忽略的。

一个规范的 cSI 方案可以通过 Fiat-Shamir 转换直接产生一个 SS 方案;如果 SI 是 imp-pa 安全的,那么转换产生的 SS 方案在随机预言模型下也是 uf-cma 安全的。可以通过下面的方法从规范的 cSI 方案 SI = ($KeyGen, P, V$)得到一个 IBS 方案:

$$IBS = (Setup, Keyder, Sing, Vf) = cSI\text{-}2\text{-}IBS(SI)$$

其中 $H: \{0,1\}^* \rightarrow Rng$ 和 $G: \{0,1\}^* \rightarrow ChSet(R)$ 是 Hash 函数。如图 2.2 所示。

方案 2.2 $IBS = cSI\text{-}2\text{-}IBS(SI)$

算法 $Setup(k)$:
  $(R,t) \leftarrow TDG(k)$; $mpk \leftarrow R$; $msk \leftarrow (R,t)$
  return (mpk, msk).
算法 $KeyDer(msk, id)$
  $(R,t) \leftarrow msk$; $x \leftarrow Inv(R,t,H(id))$
  return $usk \leftarrow (R,x)$.
算法 $Sign(usk, m)$:
  $(R,x) \leftarrow usk$; $cmt \leftarrow P(usk)$; $ch \leftarrow G(cmt \| m)$; $rsp \leftarrow P(ch)$
  return $\sigma \leftarrow (cmt, rsp)$.
算法 $Vf(mpk, id, m, \sigma)$:
  $R \leftarrow mpk$; $(cmt, rsp) \leftarrow \sigma$; $pk \leftarrow (R, H(id))$; $ch \leftarrow G(cmt \| m)$
  return $dec(pk, cmt \| ch \| rsp)$.

图 2.2 *cSI-IBE* 转换

2.2.4 分层身份方案到基于身份签名的转换(*HIBE-2-IBS* 转换)

一个深度为 d 的分层身份 $\boldsymbol{id}$ 是一个 d 元组 $\boldsymbol{id} = (id_1, \cdots, id_d)$,其中 $id_i \in \{0,1\}^*$。我们说深度为 d 的分层身份 $\boldsymbol{id}$ 是深度为 d'的分层身份 $\boldsymbol{id}'$祖先,如果 $\boldsymbol{id}$ 是 $\boldsymbol{id}'$的一个前缀,例如:对于所有的 $1 \leqslant i \leqslant d$,如果 $d \leqslant d'$并且 $id_i = id'_i$。如果 $\boldsymbol{id}$ 的深度为 0,那么它就是空字符串 ε。注:ε 是任何分级身份的祖先。

一个基于深度为 d 的分层身份加密方案是一组多项式时间算法 $HIBE = (Setup, KeyDer, Encrypt, Decrypt)$。可信的密钥分发中心运行 $Setup$ 算法,输入安全参数 k,生成密钥对(mpk, msk)。注:$\boldsymbol{id} = \varepsilon$ 的用户私钥就是主私钥 msk。身份为 $\boldsymbol{id}$ 的用户运行密钥产生算法 $KeyDer$,输入私钥 $usk_{\boldsymbol{id}}$和 $\boldsymbol{id}'$为其后代 $\boldsymbol{id}'$产生私钥(产生的私钥被认为能够安全地传送给相关的用户)。输入 $mpk, \boldsymbol{id}, M$,加密算法 Enc 返回对身份 $\boldsymbol{id}$ 的消息 m 的密文 c。输入 $usk_{\boldsymbol{id}}$和密文 c,解密算法 Dec 返回消息 m,当密文无效时返回 $\perp$。IBE 方案是深度为 1 的 HIBE 的特例。

HIBE 方案的安全性通过抵抗无特征的选择明文攻击(ind-id-cpa)来证明。本节我们只要求 HIBE 是单向抵抗选择明文攻击的(ow-id-cpa),这个较弱的概念只要求对随机密文的解密是困难的。

这种转换的思想是使用身份为 ***id*** 用户的私钥对消息 m 签名。为了更形式化地说明,假定深度为 2 并且消息空间为 $MsgSp$ 的 $HIBE = (Setup, KeyDer, Encrypt, Decrypt)$,我们建立 $IBS = (Setup, KeyDer, Sign, Vf) = HIBE\text{-}2\text{-}IBS(HIBE)$,如图 2.3 所示。

方案 2.3 $IBS = HIBE\text{-}2\text{-}IBS(HIBE)$

算法 $Sign(usk_{id}, m)$:
$id \leftarrow (id, m)$; $\sigma \leftarrow KeyDer(usk_{id}, id)$
return σ.
算法 $Vf(mpk, id, m, \sigma)$:
$id \leftarrow (id, m)$; $m' \xleftarrow{r} MsgSp$; $c \leftarrow Encrypt(mpk, id, m')$
if $Decrypt(usk_{id} = \sigma, c) = m'$ then $d \leftarrow 1$ else $d \leftarrow 0$
return d.

图 2.3 *HIBE-IBE* 转换

可以证明,如果 *HIBE* 是 ow-id-cpa 安全的,那么 HIBE-2-*IBS*(*HIBE*)是 uf-cma 安全的。和第三节中的 *cSI-2-IBS* 转换相对比,该转换并不依赖随机预言模型,所以在标准模型下是 ow-id-cpa 安全的 HIBE 方案来实例化时,就可以得到一个在标准模型下 uf-cma 安全的 IBS 方案。

2.3 Shamir 方案

Shamir 的基于身份签名方案由系统参数建立、用户密钥生成、签名及验证四部分组成,步骤如下:

(1) *Setup*:n 是两个大素数的乘积,e 是与 $\varphi(n)$ 互素的大素数,d 是满足 $ed = l(\mathrm{mod}\,\varphi(n))$ 的整数,f 是 $\{0,1\}^* \rightarrow Z_{\varphi(n)}$ 的单向 Hash 函数。PKG 的主密钥是 d,公共参数是 (n, e, f)。

(2) *Extract*:i 表示用户身份标识符。PKG 生成私钥:$g = i^d (\mathrm{mod}\, n)$。

(3) *Sign*:消息 $m \in \{0,1\}^*$,用户选择的随机数为 r 然后计算:

$$t = r^e (\mathrm{mod}\, n), \quad s = g \cdot r^{f(t \| m)} (\mathrm{mod}\, n)$$

得到签名为 (t, s)。

(4) *Verify*:输入消息 m,i 和签名 (t, s),验证如下等式:

$$s^e = i \cdot t^{f(t \| m)} (\mathrm{mod}\, n)$$

如果等式成立,则签名为有效的,否则为无效签名。

2.4 CC-IBS 方案

CC-IBS 方案，即 Cha 和 Cheon 设计的实用的基于身份的签名方案。

1. CC-IBS 签名方案描述

Setup：设 E 是定义在 F_p 上的椭圆曲线。选择一个任意的具有 q 阶的点 $P \in G_1 = E/F_p$。找到一个随机数 $s \in Z_q^*$，设置 $P_{pub} = sP$。选择 Hash 函数 $H_1: \{0,1\}^* \rightarrow G, H_2: G_2 \rightarrow \{0,1\}^n$。明文空间为 $M = \{0,1\}^n$，密文空间为 $C = G_1 \times \{0,1\}^n$。系统参数为 $params = \{p, P, P_{pub}, e, n, H_1, H_2\}$。主密钥为 $s \in Z_q$。

Extract：对于给定的字符串 $ID \in \{0,1\}^*$，建立一个私钥。映射身份到椭圆曲线上的点 $Q_{ID} = H_1(ID) \in G_1$。计算用户私钥 $d_{ID} = sQ_{ID}, s \in Z_q^*$ 为系统主私钥。

Sign：用私钥 d_{ID} 对消息 m 签名，选择一个随机串 $r \in Z_q^*$ 计算 $U = hQ_{ID}, h = H_2(m, W), V = (r+h)d_{ID}, W = rP_{pub}$，得到签名 $\sigma = \{U, V, W\}$。

Verify：为了验证用户 ID 对消息 m 的签名 σ，接收者计算 $e(P_{pub}, U)e(W, Q_{ID}) = e(P, V)$ 是否成立，其中 $h = H_2(m, W)$，如果成立，则签名有效，否则无效。

2. 安全性分析

定理 2.1 假设存在一个自适应选择消息和自适应选择身份攻击的算法 $\mathcal{A}_{\text{CC-IBS}}$，其中 $\mathcal{A}_{\text{CC-IBS}}$ 对 $H_1, H_2, Sign, Extract$ 的询问次数分别是 $q_{H_1}, q_{H_2}, q_{Sign}, q_{Extract}$，它的时间为 t_0，成功的机率为 $Adv_{\mathcal{A}_{\text{CC-IBS}}} \geqslant 10(q_s+1)(q_s+q_{H_1})q_{H_2}/(l-1)$，则 CDH 被成功解决时间为 $time \leqslant \dfrac{120686 q_{H_1} q_{H_2} t_0}{Adv_{\mathcal{A}_{\text{CC-IBS}}}\left(l - \dfrac{1}{q}\right)}$。

为了证明这个定理 2.1，首先先证明一种简化的情况：假设 CC-IBS 方案存在一个自适应选择消息和自适应选择身份攻击的算法 $\mathcal{A}_0$，算法需要的时间为 t_0，成功的机率为 $Adv_{\mathcal{A}_0}$，那么就存在自适应选择消息攻击和给定身份攻击的算法 $\mathcal{A}_1$，需要的时间为 $t_1 < t_0$，$Adv_{\mathcal{A}_1} \leqslant Adv_{\mathcal{A}_0}(l-1/q)/q_{H_2}$，其中 q_{H_2} 是 $\mathcal{A}_0$ 中对 H_2 的最大询问次数。

证明：首先任意选取 $r \in \{1, \cdots, q_{H_2}\}$，令 $\mathcal{A}_0$ 对 Hash 函数 H_2 的第 i 次询问的身份标记为 ID_i。其次运行 $\mathcal{A}_0$。用 $\mathcal{A}_1$ 来回应 $\mathcal{A}_0$ 的关于 $H_1, H_2, Sign, Extract$ 询问。然后让 $\mathcal{A}_0$ 输出 (ID_{out}, m, σ)。最后，如果 $ID_{out} = ID$，并且 (ID, m, σ) 是可用的，输出 (ID, m, σ)，其他的输出 $Fail$。

把这一攻击算法分割，可得：

$$Pr[(ID_{out}, m, \sigma) \text{ 可用}] \geqslant Adv_{\mathcal{A}_0}$$

$$Pr[ID_{out} = ID_i \mid (ID_{out}, m, \sigma) \text{ 可用}] \geqslant l - \frac{1}{q}$$

$$Pr[ID_{out} = ID_r \mid ID_{out} = ID_i] \geqslant \frac{1}{q_{H_2}}$$

通过以上的结论可得：

$$Pr[ID_{out} = ID_i = ID_r \text{ 并且}(ID,m,\sigma) \text{ 可用}] \geqslant Adv_{\mathcal{A}_0}\left(l - \frac{1}{q}\right)\frac{1}{q_{H_2}}$$

至此设计出了自适应选择消息攻击和给定身份攻击的算法 $\mathcal{A}_1$，并通过 Pointcheval 和 Stern 的理论，可以得定理 2.1。

2.5 Paterson 和 Schuldt 方案

Paterson 和 Schuldt 的签名方案是以 Waters 提出的基于身份的加密方案为基础的。在下面的论述中，设所有身份标识和消息的长度分别为 n_u, n_m 的二进制字符串。为了构造更灵活的方案，让方案中身份标识与消息长度可以是任意长度的字符串，$H_u: \{0,1\}^* \rightarrow \{0,1\}^{n_u}$，$H_m: \{0,1\}^* \rightarrow \{0,1\}^{n_m}$ 是抗碰撞的 Hash 函数，用来创建所需任意长度的身份标识和消息。定义符号 $v \leftarrow_R S$ 表示从集合 S 中随机选择出一个值 v。具体签名方案算法如下：

Setup：选择阶为素数 p 的两个群 G, G_T，构造一个满足条件的双线性映射 $e: G \times G \rightarrow G_T$，设 g 为 G 的一个生成元。选择一个保密值 $\alpha \leftarrow_R Z_p$，计算 $g_1 = g^\alpha$ 并选择 $g_2 \leftarrow_R G$。进而选择 $u', m' \leftarrow_R G$ 和向量 $\boldsymbol{u} = (u_i)$，$\boldsymbol{m} = (m_i)$，长度分别为 n_u, n_m，其中的元素为 G 中随机选出。系统的公共参数为 $params = (G, G_T, e, g, g_1, g_2, u', \boldsymbol{u}, m', \boldsymbol{m})$，主密钥为 g_2^α。

KeyDer：设身份标识 u 为一个长度为 n_u 比特的字符串，$u[i]$ 表示 u 的第 i 个比特的值。定义集合 $U \subset \{1, \cdots, n_u\}$，$u[i] = 0,1, i \in U$；构造身份 u 的私钥 d_u，选择 $r_u \leftarrow_R Z_p$ 然后计算：$d_u = \left(g_2^\alpha \left(u' \prod_{i \in U} u_i\right)^{r_u}, g^{r_u}\right)$。

Sign：设 u 为长度为 n_u 签名实体的身份标识的比特串，m 为需要签名消息的比特串。与生成密钥算法中类似，设 $U \subset \{1, \cdots, n_u\}$ 其中 $u[i] = 0,1$，同理设 $M \subset \{1, \cdots, n_m\}$ 其中 $m[j] = 0,1$，$m[j]$ 表示 m 的第 j 比特的值。身份 u 对消息 m 的签名时选择 $r_m \leftarrow_R Z_p$ 然后计算：

$$\sigma = \left(g_2^\alpha \left(u' \prod_{i \in U} u_i\right)^{r_u} \left(m' \prod_{j \in M} m_j\right)^{r_m}, g^{r_u}, g^{r_m}\right) \in G^3$$

Verify：给出身份 u 在消息 m 上的签名信息 $\sigma = (V, R_u, R_m) \in G^3$，验证者计算下面等式，相等则接受 σ：

$$e(V,g) = e(g_2, g_1) e\left(u' \prod_{i \in U} u_i, R_u\right) e\left(m' \prod_{j \in M} m_j, R_m\right)$$

很容易看出，一个利用签名算法构造的签名将会被验证者所接受。因此方

案是正确的。

安全性证明

如果计算 Diffie-Hellman 问题是困难的，则上面的基于身份的签名方案在选择消息攻击情况下是具有抗伪造性的。

定理 2.2 上面的基于身份的签名机制具有(ε,t,q_e,q_s)安全性——在 t 时间内敌手进行 q_e 次密钥生成查询和 q_s 次签名查询后敌手的优势为 ε，则在群 G 中进行(ε',t')-CDH 假设，其中 $\varepsilon' = \dfrac{\varepsilon}{16(q_e+q_s)q_s(n_u+1)(n_m+1)}$，$t' = t + O((q_e n_u + q_s(n_u+n_m))\rho + (q_e+q_s)\tau)$，$\rho,\tau$ 分别代表群 G 中乘法与乘方运算。

证明：假设方案中存在一个(ε,t,q_e,q_s)伪造者 $\mathcal{A}$，从这个伪造者这里，可以构造一个至少拥有概率 ε'和至多用 t'时间来解决 CDH 问题的算法 $\mathcal{B}$，用这个算法来反驳(ε',t')-CDH 假设。算法 $\mathcal{B}$ 给出一个群 G，一个生成元 g 以及元素 g^a，g^b。为了能用 $\mathcal{A}$ 来计算 g^{ab}，$\mathcal{B}$ 必须能够为 $\mathcal{A}$ 模拟一个挑战者。按照以下的方法进行模拟：

系统建立：$\mathcal{B}$ 设 $l_u = 2(q_e+q_s)$ 和 $l_m = 2q_s$，然后随机选择两个整数 k_u,k_m，满足 $0 \leqslant k_u \leqslant n_u$，$0 \leqslant k_m \leqslant n_m$。设给定的值 q_e,q_s,n_u,n_m 满足条件 $l_u(n_u+1) < p$ 以及 $l_m(n_m+1) < p$。模拟者选定一个整数 $x' \leftarrow_R Z_{l_u}$ 和一个长度为 n_u 的向量 $\boldsymbol{x} = (x_i)$，其中 x_i 满足 $x_i \leftarrow_R Z_{l_u}$。同样的，随机选择另一个整数 $z' \leftarrow_R Z_{l_m}$ 和长度为 n_m 的向量 $\boldsymbol{z} = (z_j)$ 其中 z_j 满足 $z_j \leftarrow_R Z_{l_m}$。最后，$\mathcal{B}$ 选择两个整数 $y',w' \leftarrow_R Z_p$ 和两个长度分别为 n_u,n_m 向量，$\boldsymbol{y} = (y_i)$，$\boldsymbol{w} = (w_j)$，其中 y_i,w_j 满足 $y_i,w_j \leftarrow_R Z_p$。为了使描述更简单，分别为身份 u 和消息 m 定义如下两对函数：

$$F(u) = x' + \sum_{i \in U} x_i - l_u k_u \text{ 和 } J(u) = y' + \sum_{i \in U} y_i$$

$$K(m) = z' + \sum_{j \in M} z_j - l_m k_m \text{ 和 } L(m) = w' + \sum_{j \in M} w_j$$

现在 $\mathcal{B}$ 通过如下方式构建了为 IBE 方案使用的公共参数集合：

$$g_1 = g^a, g_2 = g^b$$

$$u' = g_2^{-l_u k_u + x'} g^{y'}, \quad u_i = g_2^{x_i} g^{y_i}, \quad 1 \leqslant i \leqslant n_u$$

$$m' = g_2^{-l_m k_m + z'} g^{w'}, \quad m_j = g_2^{z_j} g^{w_j}, \quad 1 \leqslant j \leqslant n_m$$

注意这些公共参数在挑战者与 $\mathcal{A}$ 之间的分配是一致的。进而，主秘密值为 $g_2^a = g_2^a = g^{ab}$，在身份 u 和消息 m 之间满足以下等式：

$$u' \prod_{i \in U} u_i = g_2^{F(u)} g^{J(u)}, \quad m' \prod_{j \in M} m_j = g_2^{K(m)} g^{L(m)}$$

所有的公共参数被传递给 $\mathcal{A}$。

查询过程：当运行攻击时就会产生生成查询和签名查询。

$\mathcal{B}$ 按照如下方式回复查询信息：

密钥生成查询:一个对于身份 u 私钥的查询,$\mathcal{B}$ 不知道主秘密值,但是假设 $F(u)\neq 0 \pmod p$,通过选择 $r_u \leftarrow_R Z_p$ 和如下计算能够构建一个私钥:

$$d_u = (d_0, d_1) = \left(g_1^{-J(u)/F(u)}\left(u'\prod_{i\in U} u_i\right)^{r_u}, g_1^{-1/F(u)} g^{r_u}\right)$$

设 $\tilde{r_u} = r_u - a/F(v)$,用这种方式定义 d_u 生成一个身份 u 可用的私钥,证明如下:

$$\begin{aligned} d_0 &= g_1^{-J(u)/F(u)}\left(u'\prod_{i\in U} u_i\right)^{r_u} \\ &= g_2^a\left(g_2^{F(u)} g^{J(u)}\right)^{-a/F(u)}\left(g_2^{F(u)} g^{J(u)}\right)^{r_u} \\ &= g_2^a\left(g_2^{F(u)} g^{J(u)}\right)^{r_u - a/F(u)} \\ &= g_2^a\left(u'\prod_{i\in U} u_i\right)^{\tilde{r_u}} \end{aligned}$$

并且 $d_1 = g_1^{-1/F(u)} g^{r_u} = g^{r_u - a/F(u)} = g^{\tilde{r_u}}$。

因此为了攻击,所有由 $\mathcal{B}$ 计算产生的私钥均与真正的调整者生成的密钥不同。

另一方面,如果 $F(u) = 0 \pmod p$,以上的计算过程不能被执行并且模拟者会终止模拟。为了使模拟分析更容易,当 $F(u) = 0 \pmod{l_u}$ 时将强制模拟终止。由假设条件 $l_u(n_u + 1) < p$,可推出 $0 \leqslant l_u k_u < p, 0 \leqslant x' + \sum_{i\in U} x_i < p$。很容易看出,若 $F(u) = 0 \pmod p$ 则 $F(u) = 0 \pmod{l_u}$。因此,由 $F(u) \neq 0 \pmod p$ 可得 $F(u) \neq 0 \pmod{l_u}$,这样刚才的条件就完全满足了确保可以成功地构建身份 u 的私钥。

签名查询:一个对身份 u 在消息 m(在没有失去普遍意义的条件下,假设 $\mathcal{A}$ 没有产生对身份 u 的查询信息)上签名的查询。如果 $F(u) \neq 0 \pmod{l_u}$,$\mathcal{B}$ 仅能在一个生成查询中为身份 u 构建一个私钥,同时使用签名算法来创建一个对消息 m 的签名。

如果 $F(u) = 0 \pmod{l_u}$,$\mathcal{B}$ 将尝试用同样的方式在生成查询中构建一个私钥。假设 $K(m) \neq 0 \pmod{l_m}$,同上文讨论的,在假设条件 $l_m(n_m + 1) < p$ 下可以得出 $K(m) \neq 0 \pmod p$。身份 u 在消息 m 上的签名可以利用如下计算并随机选择 $r_u, r_m \leftarrow_R Z_p$ 得出:

$$\sigma = \left(\left(u'\prod_{i\in U} u_i\right)^{r_u} g_1^{-L(m)/K(m)}\left(m'\prod_{j\in M} m_i\right)^{r_m}, g^{r_u}, g_1^{-1/K(m)} g^{r_m}\right)$$

$$= \left(g_2{}^a\left(u'\prod_{i\in U} u_i\right)^{r_u}\left(m'\prod_{j\in M} m_j\right)^{\tilde{r_m}}, g^{r_u}, g^{\tilde{r_m}}\right)$$

其中 $\tilde{r_m} = r_m - a/K(m)$。最后的等式表明了 $\mathcal{B}$ 发出了对 $\mathcal{A}$ 签名的回复,就像他们和一个真正的挑战者通信一样。

如果 $K(m) = 0 \pmod{l_m}$,则模拟被终止。

伪造过程：如果 $\mathcal{B}$ 在上面的模拟过程没有被终止，$\mathcal{A}$ 就会存在至少 ε 的概率获得一个身份 u^* 和一条消息 m^* 以及一个可用的伪造一个身份 u^* 在消息 m^* 上的签名 $\sigma^* = (V, R_u, R_m)$。如果 $F(u^*) \neq 0 \pmod p$ 或者 $K(m^*) \neq 0 \pmod p$，那么 $\mathcal{B}$ 就会终止。另一方面，如果 $F(u^*) = 0 \pmod p$ 和 $K(m^*) = 0 \pmod p$，$\mathcal{B}$ 会计算并输出：

$$\frac{V}{R_u^{J(u^*)} R_m^{L(m^*)}} = \frac{g_2^{\alpha} \left(u' \prod_{i \in U} u_i\right)^{r_u} \left(m' \prod_{j \in M} m_i\right)^{r_m}}{g_1^{J(u^*) r_u} g^{L(m^*) r_m}} = g^{ab}$$

并以此来解决给定的 CDH 问题。

以上就完成了对模拟过程的描述。仍然需要分析 $\mathcal{B}$ 终止的概率。为了能使模拟过程没有终止，要求所有对于身份 u 的生成查询必须满足 $F(u) \neq 0 \pmod{l_u}$ 并且所有的签名查询必须满足 $F(u) \neq 0 \pmod{l_u}$ 或者 $K(u) \neq 0 \pmod{l_m}$，并且 $F(u^*) = 0 \pmod{l_u}$ 和 $K(m^*) = 0 \pmod{l_m}$。然而，为了让分析过程变得更简单，要对这种事件的子情况进行限制。更具体地说，可以将签名查询分为两个部分，一个部分查询包括 u^*，另一部分查询的身份 $u \neq u^*$，然后考虑所有身份 u 都满足 $F(u) \neq 0 \pmod{l_u}$ 的情况，忽略对 (u, m) 的签名查询在 $F(u) = 0 \pmod{l_u}$ 和 $K(m) = 0 \pmod{l_m}$ 条件下的应答。这样对 $\mathcal{B}$ 终止的概率就会降低限制。

设 $u_1, \cdots, u_{q_I}$ 为生成查询中出现的身份，或者签名查询出现的身份但是不包括挑战者的身份。设 $m_1, \cdots, m_{q_M}$ 为包括挑战者身份 u^* 的签名查询的消息。可以很清楚的得出 $q_I \leqslant q_e + q_s$，$q_M \leqslant q_s$。定义事件 A_i, A^*, B_j, B^* 为：

$$A_i : F(u_i) \neq 0 \pmod{l_u}$$

$$A^* : F(u_i) = 0 \pmod p$$

$$B_j : K(m_j) \neq 0 \pmod{l_m}$$

$$B^* : K(m^*) = 0 \pmod p$$

从上面的分析可知 $\mathcal{B}$ 没有终止的概率为：

$$Pr[\neg\, abort] \geqslant Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{j=1}^{q_M} B_j \wedge B^*\right]$$

很容易看出事件 $\left(\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right)$ 和事件 $\left(\bigwedge_{j=1}^{q_M} B_j \wedge B^*\right)$ 是相互独立的。本质上这是因为过程 F 和 K 定义的事件是被选择出的独立的事件，而且从敌手的简单来看模拟过程 F 和 K 是透明的。

如上所述，假设条件 $l_u(n_u + 1) < p$ 暗含了 $F(u) = 0 \pmod p \Rightarrow F(u) = 0 \pmod{l_u}$。进而，如果 $F(u) = 0 \pmod{l_u}$，则在 $0 \leqslant k_u \leqslant n_u$ 范围内对 k_u 存在唯一的选择使得 $F(u) = 0 \pmod p$。因为 k_u 和 $x', \boldsymbol{x}$ 是随机选择的，所以可得：

$$Pr[A^*] = Pr[F(u^*) = 0 \pmod p \wedge F(u^*) = 0 \pmod{l_u}]$$

$$= Pr[F(u^*) = 0 \pmod{l_u}]Pr[F(u^*) = (0 \bmod p) \mid F(u^*) = 0 \pmod{l_u}] = \frac{1}{l_u}\frac{1}{n_u + 1}$$

还可以推出：

$$Pr\left[\bigwedge_{i=1}^{q_I} A_i \mid A^*\right] = 1 - Pr\left[\bigvee_{i=1}^{q_I} A_i \mid A^*\right] \geqslant 1 - \sum_{i=1}^{q_I} Pr[\neg A_i \mid A^*]$$

对两个不同身份 u_1, u_2，由于至少存在一个随机选择值，则 $F(u_1), F(u_2)$ 将会不同，从而事件 $F(u_1) = 0 \pmod{l_u}, F(u_2) = 0 \pmod{l_u}$ 将会是独立的。具体来讲，对于任何值 i，事件 A_i, A^* 是相互独立的，并且 $Pr[\neg A_i \mid A^*] = 1/l_u$，因此

$$Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right] = Pr[A^*]Pr\left[\bigwedge_{i=1}^{q_I} A_i \mid A^*\right] \geqslant \frac{1}{l_u(n_u + 1)}\left(1 - \frac{q_e + q_s}{l_u}\right)$$

设 $l_u = 2(q_e + q_s)$ 则有

$$Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right] \geqslant \frac{1}{4(q_e + q_s)(n_u + 1)}$$

模拟者通过分析签名查询然后给出结果

$$Pr\left[\bigwedge_{j=1}^{q_M} B_j \wedge B^*\right] \geqslant \frac{1}{4q_s(n_m + 1)}$$

从而可以得到

$$Pr[\neg abort] \geqslant Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right]Pr\left[\bigwedge_{j=1}^{q_M} B_j \wedge B^*\right] \geqslant \frac{1}{16(q_e + q_s)q_s(n_u + 1)(n_m + 1)}$$

如果模拟过程没有终止，那么 $\mathcal{A}$ 有至少 ε 的概率伪造出一个可用的签名。算法 $\mathcal{B}$ 会按照上述方法从伪造的签名计算出 g^{ab}。

算法 $\mathcal{B}$ 的时间复杂度由乘方运算决定，以及对于较大值 n_u, n_m 在生成查询和签名查询中的乘法运算决定。由于在生成查询和签名查询阶段乘法运算的复杂度分别为 $O(n_u), O(n_u + n_m)$，乘方运算的复杂度分别为 $O(1), O(1)$，所以算法 $\mathcal{B}$ 的时间复杂度为 $t + O((q_e n_u + q_s(n_u + n_m))\rho + (q_e + q_s)\tau)$。因此定理得证。

2.6 Hu 和 Li 等人的方案

设 G, G_1 和 G_T 是具有 p 阶的群，双线性影射为 $e: G \times G_1 \rightarrow G_T$。

Setup:随机产生 g 作为 G 的生成元,$g_1=\psi(g)$(ψ 表示同构),$h,h_1\xleftarrow{R}G_1$,$u=h_1^{\alpha}$,$v=g^{\alpha}$。签名方案的公共参数和主密钥分别是:$params=(g,g_1,h,h_1,u,v)$,$master-key=\alpha$。

Extract:生成对应身份 $ID\in Z_p$ 的私钥,PKG 生成 $r_{ID}\xleftarrow{R}Z_p$,输出私钥 d_{ID}:$d_{ID}=(d_1,d_2)$,其中 $d_1=(hg_1^{-r_{ID}})^{1/\alpha-ID}$,$d_2=r_{ID}$。

Sign:需要签名的消息为 $m\in Z_p$,用户签名的身份为 ID,用户随机选取 $s\in Z_p$,并产生签名 σ:$\sigma=(\sigma_1,\sigma_2,\sigma_3)$,其中 $\sigma_1=d_1(uh_1^{-ID})^{(r_{ID}+s)m}$,$\sigma_2=(vg^{-ID})^{r_{ID}+s}$,$\sigma_3=d_2=r_{ID}$。

Verify:为了验证发送用户 ID 关于消息 m 的签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$,接收用户计算下面的等式是否成立:$e(vg^{-ID},\sigma_1)=e(g,h)e(g,g_1)^{-r_{ID}}e(\sigma_2,(uh_1^{-ID})^m)$。如果成立,说明签名有效,输出 *accept*;否则签名无效,输出 *reject*。

可行性分析:

可行性分析将通过下面的推导进行证明:

$$\begin{aligned}e(vg^{-ID},\sigma)&=e(g^{\alpha-ID},d_1(uh_1^{-ID})^{m(r_{ID}+s)})\\&=e(g^{\alpha-ID},(hg_1^{-r_{ID}})^{1/\alpha-ID})e(g^{\alpha-ID},(uh_1^{-ID})^{m(r_{ID}+s)})\\&=e(g,hg_1^{-r_{ID}})e(\sigma_2,(uh_1^{-ID})^m)\\&=e(g,h)e(g,g_1)^{-r_{ID}}e(\sigma_2,(uh_1^{-ID})^m)\end{aligned}$$

等式的成立,是设计方案的关键问题,保证了用户可以验证消息是否被篡改,或签名是否有效。

安全性分析:

定理 2.3 如果(t,e,q)-SDH 假设是成立的,那么这个方案在条件(t',q_e,q_s,e')下是 EU-ID-CMA 安全的,记作(t',q_e,q_s,e')-EU-ID-CMA,其中 $q=q_e+1$,$t'=t-o(t_{\exp}\cdot q(q+q_s))$,$e'=e+(1-qq_e/p)(1-qq_s/p)(1-q/p)$,$t_{\exp}$表示群上一次幂运算的时间。

证明:假设对本方案存在一个(t',q_e,q_s,e')的伪造算法 $\mathcal{A}$,可以利用 $\mathcal{A}$ 构造算法 $\mathcal{B}$ 用于解决 q-SDH 问题。

向量$(g,g_1,g_2,\cdots,g_q)$作为 $\mathcal{B}$ 解决 q-SDH 问题的输入,其中 $g_i=g_1^{\alpha^i}$。$\mathcal{B}$ 通过下面的方法来模拟 $\mathcal{A}$ 的攻击。

系统建立:$\mathcal{B}$ 生成一个多项式 $f(x)\in Z_p[x]$,最高次幂为 q,设 $h=g_1^{f(\alpha)}$,随机地给定 $\mu\in_R Z_p$,让 $h_1=g_1^{\mu}$,$u=(\psi(v))^{\mu}$,公开 $params=(g,g_1,h,h_1,u,v)$。

查询:攻击者提出 *Extract* 和 *Sign* 询问时,$\mathcal{B}$ 按照以下的方法答复:

—密钥生成查询:对身份 I 私钥的询问,如果 $I=\alpha$,$\mathcal{B}$ 就可以直接解决 q-SDH 难题。否则,构造一个$(q-1)$次的多项式 $F(x)=(f(x)-f(I))/(x-I)$,

得到身份 I 的私钥：$d_1 = g_1^{F(\alpha)}$，$d_2 = r = f(I)$，如果 $r = 0$，则 $\mathcal{B}$ 中断。

—签名查询：攻击者进行签名询问，要签名的消息 m，签名的身份为 I，这个过程与 *Extract query* 相似：$\sigma = (g_1^{F(\alpha)}(uh_1^{-I})^{(f(I)+f(m))m}, (vg^{-I})^{f(I)+f(m)}, f(I))$，如果 $f(I) = 0$，则 $\mathcal{B}$ 中断。

—伪造过程：在以上的过程中，$\mathcal{B}$ 没有中断，攻击者产生了一个有效的签名 $\sigma^* = (\sigma_1^*, \sigma_2^*, r^*)$，签名的身份是 I^*，签名的消息是 m^*。如果 $r^* = 0$，$\mathcal{B}$ 中断，否则通过计算：$W = \dfrac{\sigma_1^*}{\psi(\sigma_2^*)^{m\mu}} = g^{(f(\alpha)-r^*)/(\alpha-I^*)}$，$g^{1/(\alpha-I^*)} = \dfrac{W}{g^{F(\alpha)(\alpha-I^*)}}$，$\mathcal{B}$ 输出 $(g^{1/(\alpha-I^*)}, I^*)$ 作为 q-SDH 难题的结果。这是与定理 2.3 相矛盾的。

通过以上的攻击模拟，根据[27]中的证明，对出现中断的概率进行分析。因为 $f(x)$ 在 Z_p 上是随机分布的，所以由 $\mathcal{B}$ 产生的参数在概率上是独立的。对任意输入的 x 使得 $f(x) = 0$ 的概率是 q/p，q 为 $f(x)$ 解的个数。因此 $\mathcal{B}$ 不发生中断的概率为 $(1 - qq_e/p)(1 - qq_s/p)(1 - q/p)$。

2.7 Narayan 和 Parampalli 方案

本节描述了 Narayan 和 Parampalli 提出的两种不需要随机预言构造安全签名方案的设计。第一个方案是指定一名特定的接收者，当第三方不具有特定接收者身份时无法验证消息及其签名的真伪。第二个方案是第一个方案的变体，该方案中的消息及其签名可以被公共域内已知该消息发送者的所有用户检验其真伪。

方案 1：指定接收者验证的签名

方案 1 构造一个提供验证消息发送者并可以指定特定接收者的签名方案。该方案不但可以保证消息发送方的真实身份，同时提供了对接收者身份的限定。

Setup：PKG 选择两个阶为素数 q 的群 G_1 和 G_2，其中 G_1 的生成元为 g，并满足双线性映射 $e: G_1 \times G_1 \to G_2$。然后 PKG 随机选择一个秘密值 $s \in Z_q^*$，计算 $g_1 = g^s$ 同时选择 $g_2 \in_R G_1$。进一步 PKG 选择 $u', u'_m \in_R G_1$，选择 $\boldsymbol{u} = (u_i)$ 为 n 维向量，其中的各个分量由 G_1 中随机选出的元素组成。

抗强碰撞的函数 $H_u: \{0,1\}^n \to G$ 设计如下：设身份变量 u，使 $U \subseteq \{1, \cdots, n\}$，$u[i]$ 代表身份字符串中第 i 个比特值，对于一个身份 u：

$$H_u(u) = u' \prod_{i \in U} u_i$$

函数 $H_{m''}: \{0,1\}^n \to G$ 设计如下：给定消息二进制字符串为 m''，使用 $M \subseteq \{1, \cdots, n\}$ 代表消息字符串的集合，其中 $m''[j]$ 代表消息字符串集合中的第 j 个元素，则

$$H_{m''}(m'') = u'_m \prod_{j \in M} u_j$$

另外，PKG 选择一个抗碰撞 Hash 函数 $H_m: \{0,1\}^* \times G_1 \rightarrow Z_q^*$ 将一个任意长度的消息映射到一个整数。系统的参数如下：$params = (g, g_1, g_2, u', u'_m, \boldsymbol{u}, H_m, H_u, H_{m''})$，主秘密值为 g_2^s。

Extract：给定一个身份 u，生成算法生成私钥 d_u：

（1）$r_u \in_R Z_q^*$，对于每一个身份这个值都是唯一的；

（2）私钥为 $d_u = (g_2^s \cdot g_u^{r_u}, g^{r_u})$，其中 $g_u = H_u(u)$ 是 u 的公钥。

Sign：给定一个消息 m，发送者标识为 u_s，接受者标识为 u_r，u_s 在消息 m 上的签名构造过程如下：

（1）选择 $t \in_R Z_q^*$；

（2）计算 $m' = H_m(m, g^{r_{u_s}})$；

（3）m''为 m'的二进制字符串，$g_{m''} = H_{m''}(m'')$；

（4）计算 $Z = (g_{m''} g_{u'})^{tm'} \cdot g_2^s \cdot g_{u_s}^{r_{u_s}}$；

（5）签名为$(Z, U = g^t, V = g^{r_{u_s}})$。

Verify：在消息 m 上的签名为(Z, U, V)，验证过程如下：

（1）$m' = H_m(m, g^{r_{u_s}})$；

（2）m''为 m'的二进制字符串，$g_{m''} = H_{m''}(m'')$；

（3）接受签名的条件：$e(g, Z) = e(U, g_{u_r} g_{m''})^{m'} \cdot e(g_1, g_2) \cdot e(V, g_{u_s})$。

验证算法的正确性：

考虑上面的验证算法，利用双线性对的性质将 $e(g, Z)$表示如下：

$$e(g, Z) = e(g, (g_{m''} g_{u_r})^{tm'}) \cdot e(g_1, g_2^s) \cdot e(g, g_{u_s}^{r_{u_s}})$$

$$e(g, Z) = e(g^t, (g_{m''} g_{u_r})^{m'}) \cdot e(g^s, g_2) \cdot e(g^{r_{u_s}}, g_{u_s})$$

$$e(g, Z) = e(U, (g_{u_r} g_{m''})^{m'}) \cdot e(g_1, g_2) \cdot e(V, g_{u_s})$$

代入验证等式可证明其正确。

验证签名的过程中需要将接受者的身份作为输入参数之一。如果接收者身份被隐藏在签名中（例如签名被通过私有信道传递给接收者），第三方则不能验证签名。因此，签名方案 1 可以指定特定的接收者。

方案 2

方案 2 由方案 1 演变而来。具体如下：

Setup：同方案 1 系统建立过程。

Extract：同方案 1 生成算法。

Sign：给定一个消息 m，发送者标识为 u_s，接受者标识为 u_r，在 u_s 消息 m 上的签名构造过程如下：

(1) 选择 $t \in_R Z_q^*$;

(2) 计算 $m' = H_m(m, g^{r_{u_s}})$;

(3) m''为 m'的二进制字符串;

(4) 计算 $g_{m''} = H_{m''}(m'')$;

(5) 计算 $Z = (g_{u_s} \cdot g_{m''})^{tm'} \cdot g_2^s \cdot g_{u_s}^{r_{u_s}}$;

(6) 签名是:$(Z, U = g^t, V = g^{r_{u_s}})$。

Verify:在消息 m 上的签名为(Z, U, V),验证过程如下:

(1) 计算 $m' = H_m(m, g^{r_{u_s}})$;

(2) m''为 m'的二进制字符串;

(3) 计算 $g_{m''} = H_{m''}(m'')$;

(4) 接受签名的条件 $e(g, Z) = e(g_1, g_2) \cdot e(U^{m'}, g_{u_s} \cdot g_{m''}) \cdot e(V, g_{u_s})$。

验证算法的正确性:

利用签名算法在消息 m 上的签名为(Z, U, V),利用双线性对的性质将 $e(g, Z)$表示如下:

$$e(g,Z) = e(g,(g_{m''}g_{u_s})^{tm'}) \cdot e(g_1,g_2^s) \cdot e(g,g_{u_s}^{r_{u_s}})$$

$$e(g,Z) = e(g^t,(g_{m''}g_{u_r})^{m'}) \cdot e(g^s,g_2) \cdot e(g^{r_{u_s}},g_{u_s})$$

$$e(g,Z) = e(U^{m'},g_{m''}g_{u_s}) \cdot e(g_1,g_2) \cdot e(V,g_{u_s})$$

将上述三个等式代入验证等式可证明其正确。

方案 1 的安全性证明

定理 2.4 设 $Adv_{TCR,H}^{Hash\text{-}tcr}(k)$为敌手 $\mathcal{A}$ 攻击 H_m 抗碰撞性的优势。假设存在 $a \in (\varepsilon, t, Q_e, Q_s)$-$\mathcal{A}$,这样伪造者就可以破坏掉方案 1 的 EUF-IDS-CMA 性质,然后挑战者 $\mathcal{B}$ 在 t'时间内计算出至少一个 $\varepsilon' = \varepsilon/(8(n+1)(Q_e+Q_s)^2(1 - Adv_{TCR,H}^{Hash\text{-}tcr}(k))$,$t' = t + O((Q_e \cdot n + Q_s \cdot n)\rho + (Q_e + Q_s)\tau)$,这样就可以找到一个碰撞点 Pr 从而解决 CDH 问题。

证明:敌手 $\mathcal{A}$ 在选择消息攻击的情况下具有的优势设为$(\varepsilon, t, Q_e, Q_s)$,挑战者 $\mathcal{B}$ 从敌手处了解到一个与(t', ε')-CDH 假设相矛盾的优势 ε'来构建攻击。挑战者计算出群 G_1 的生成元 g 和 CDH 问题中的 g^a 和 g^b,然后从敌手 $\mathcal{A}$ 处得到解决 CDH 问题的关键元素 g^{ab}。最后挑战者必须模拟真实环境来进行攻击,从而可以高效地回答 $\mathcal{A}$ 的查询信息,但过程中必须避免模拟环境异常终止。这样的模拟流程可以按一下方法创建。

系统建立:挑战者设变量 $\theta = 2(Q_e + Q_s)$,其中 Q_e,Q_s 分别为生成查询信息的最大数目和签名语言。n 代表身份和消息的长度;挑战者选择 $l \in_R Z_n$。假设 $\theta(n+1) < q$,设置好 Q_e,Q_s 和 n 的值,选择 $x', x_\theta' \in_R Z_\theta$ 和长度为 n 的随机向量 $\boldsymbol{x} = (x_i)$,其中的元素从 0 到 $\theta - 1$ 之间的整数中随机生成。另外挑战者随机选

择 $y', y'_\theta \in Z_q$ 和长度为 n 的向量 $\boldsymbol{y} = (y_i)$，其中向量的分量在 Z_q 中随机产生。这些变量的值在模拟过程的内部保存，不作为公共参数的一部分。

对于身份 u 定义如下函数：

$$F(u) = x' + \sum_{i \in U} x_i - \theta l \tag{1}$$

$$J(u) = y' + \sum_{i \in U} y_i \tag{2}$$

其中 $U \subseteq \{1, \cdots, n\}$ 表示所有元素 i 组成的集合。

设 m'' 为 m' 的二进制字符串，定义如下函数：

$$K(m'') = x'_\theta + \sum_{j \in M} x_j - \theta l \tag{3}$$

$$L(m'') = y'_\theta + \sum_{j \in M} y_j \tag{4}$$

其中 $M \subseteq \{1, \cdots, n\}$ 表示所有元素 j 组成的集合。

$\mathcal{B}$ 构建一个公共参数集合，传递给敌手 $\mathcal{A}$，具体参数如下：

$$g_1 = g^a, g_2 = g^b$$

$$u' = g^{-\theta l + x'} \cdot g^{y'}$$

$$u'_m = g_2^{-\theta l + x'_m} \cdot g^{y'_m}$$

$$u_i = g_2^{x_i} \cdot g^{y_i}$$

上述公共参数由 $\mathcal{A}$ 和 $\mathcal{B}$ 采用统一的随机算法生成。方案中的主秘密值为 $g_2^a = g^{ab}$。公钥按照以下流程生成：

$$g_u = u' \prod_{i \in U} u_i = g_2^{-\theta l + x'} \cdot g^{y'} \cdot \prod_{i \in U} g_2^{x_i} \cdot g^{y_i}$$

$$g_u = g_2^{x' - \theta l + \sum_{i \in U} x_i} \cdot g^{y' + \sum_{i \in U} y_i}$$

$$g_u = g_2^{F(u)} g^{J(u)}$$

注：当 $F(u) = 0 \pmod q$，身份 u 的公钥通过 $g_u = g^{J(u)}$。当 $K(m'') = 0 \pmod q$ 时，存在 $g_{m''} = g^{L(m'')}$。

查询阶段：在查询阶段中，要求敌手 $\mathcal{A}$ 生成签名查询，$\mathcal{B}$ 对 $\mathcal{A}$ 进行的查询进行回复。

密钥生成查询：$\mathcal{B}$ 不知道这次模拟中的秘密值，然而假设 $F(u) \neq 0 \pmod q$，可以选择 $r_u \in_R Z_q$ 并利用下面等式构建出私钥：

$$d_u = (d_u[0], d_u[1]) = (g_1^{-J(u)/F(u)} \cdot g_u^{r_u}, g_1^{-1/F(u)} \cdot g^{r_u})$$

另 $\bar{r}_u = r_u - (a/F(u))$，$u$ 的有效私钥按照上个等式构建出的结果为

$$d_u[0] = g_1^{-J(u)/F(u)} \cdot g_u^{r_u}$$

$$d_u[0] = g_2^a \cdot (g_2^{F(u)} \cdot g^{J(u)})^{-a/F(u)} \cdot g_u^{r_u}$$

$$d_u[0] = g_2^a \cdot (g_u)^{-a/F(u)} \cdot g_u^{r_u}$$

$$d_u[0] = g_2^a \cdot g_u^{\tilde{r}_u}$$

$$d_u[1] = g_1^{-1/F(u)} \cdot g^{r_u}$$

$$d_u[1] = g^{-a/F(u)} \cdot g^{r_u} = g^{\tilde{r}_u}$$

从而,构建的密钥 $d_u = (d_u[0], d_u[1])$ 即成为身份 u 的有效的私钥。

$\mathcal{B}$ 可以为除了 $F(u) = 0 \pmod q$ 的所有身份构建私钥,只有 $F(u) = 0 \pmod q$ 的情况发生时,模拟过程才会终止。模拟过程的前提条件即为 $F(u) = 0 \pmod m$ 时,模拟过程将终止。由于 $\theta(n+1) < q$ 则有 $0 \leqslant \theta l < q$ 和 $0 \leqslant x' + \sum_{i \in U} x_i < q$,很明显由 $F(u) = 0 \pmod q$ 可以推出 $F(u) = 0 \pmod \theta$。同理由 $K(m'') = 0 \pmod q$ 得 $K(m'') = 0 \pmod \theta$。

签名查询:设发送者的身份为 u_s,接收者的身份为 u_r。在进行 u_s 发送给 u_r 的消息(m)的签名查询时,$\mathcal{A}$ 不能对身份 u_s 的签名查询。

如果 $F(u_s) \neq 0 \pmod \theta$,则 $\mathcal{B}$ 能构建出对于身份 u_s 的私钥,然后利用如下过程生成 u_s 身份的签名:

(1) $t \in_R Z_q^*$;

(2) $m' = H_m(m, g^{\tilde{r}_{u_s}})$;

(3) 设 m'' 为 m' 的二进制字符串,$g_{m''} = H_{m''}(m'')$;

(4) $Z = (g_{m''} \cdot g_{u_r})^{tm'} \cdot g_2^a \cdot g_{u_s}^{\tilde{r}_{u_s}}$;

(5) 签名结果为 $(Z, U = g^t, V = g^{\tilde{r}_{u_s}})$。

在 $F(u_s) \neq 0 \pmod \theta$ 和 $F(u_r) \neq 0 \pmod \theta$ 条件下,按照以下过程模拟:

(1) 由于 $F(u_r) \neq 0 \pmod \theta$ 则构造出 u_r 的私钥 $(g_2^a, g_{u_r}^{\tilde{r}_{u_s}}, g_{u_r}^{\tilde{r}_{u_s}})$;

(2) 选择 $t \in_R Z_q^*$;

(3) $m' = H_m(m, g^t)$,m'' 为 m' 的二进制字符串;

(4) 如果 $K(m'') = 0 \pmod \theta$ 则进行下一步,否则转到步骤 2;

(5) $g_{m''} = H_{m''}(m'')$;

(6) $Z = (g^t)^{J(u_s)} \cdot g_2^a \cdot g_{u_r}^{\tilde{r}_{u_r}} \cdot (g^{\tilde{r}_{u_r}})^{L(m'')}$;

(7) 签名结果为 $(Z, U = g^{\tilde{r}_{u_r} M'^{-1}}, V = g^t)$。

注:上一种情况中,g^t 的值对于每一个发送者身份 u_s 是一致的。这是因为在方案中 g^{r_A} 对于身份 A 是固定不变的(密钥生成的真实性保证的),为了在模拟过程中保持一致性,模拟者必须能够复制密钥生成函数的功能。

在 $F(u_s) = 0 \pmod \theta$ 和 $F(u_r) = 0 \pmod \theta$ 的条件下,模拟过程如下:

(1) 选择 $t \in_R Z_q^*$;

(2) $m' = H_m(m, g^t)$,m'' 为 m' 的二进制字符串;

(3) 如果 $K(m'') \neq 0 (\mathrm{mod}\ \theta)$,则进行下一步,否则进行步骤 1;

(4) $g_{m^*} = H_{m^*}(m'')$;

(5) 为 m''构建的私钥为$(g_2^a, g_{m''}^{\bar{r}_{m''}}, g^{\bar{r}_{m''}})$;

(6) $Z = g^{\bar{r}_{m''} J(u_r)} \cdot (g_{m''}^{\bar{r}_{m''}}) \cdot g_2^a \cdot (g^t)^{J(u_s)}$;

(7) 签名结果为$(Z, U = g^{\bar{r}_{m''} m' + 1}, V = g^t)$。

当 $F(u_r) = 0 (\mathrm{mod}\ q)$, $K(m'') = 0 (\mathrm{mod}\ \theta)$, $F(u_s) = 0 (\mathrm{mod}\ q)$时,模拟过程终止。

伪造过程:当 $\mathscr{B}$ 没有终止时,敌手将会利用 $Pr\varepsilon$ 返回一组值(u_s^*, m^*, c^*, u_r^*),其中 $c^* = (Z, A = g^t, B = g^{\bar{r}_{u_s^*}})$,一个可用的伪造签名$(u_s^*, m^*)$。如果 $F(u_s^*) \neq 0 (\mathrm{mod}\ q)$或者 $F(u_r^*) \neq 0 (\mathrm{mod}\ q)$或者 $K(m''^*) \neq 0 (\mathrm{mod}\ \theta)$,则 $\mathscr{B}$ 会终止过程。如果 $F(u_s^*) = 0 (\mathrm{mod}\ q)$, $K(m''^*) = 0 (\mathrm{mod}\ \theta)$和 $F(u_r^*) = 0 (\mathrm{mod}\ q)$,则 $\mathscr{B}$ 可以用下面给出的等式解决 CDH 难题:

$$\frac{Z}{A^{L(m''^*)m'} \cdot A^{J(u_r^*)m'} \cdot B^{J(u_s^*)}} = \frac{g_2^a \cdot g_{u_s^*}^{\bar{r}_{u_s^*}} \cdot (g_{m''^*} g_{u_r^*})^{m' \cdot t}}{(g_{m''^*})^{M't} \cdot g_{u_s^*}^{\bar{r}_{u_s^*}}} = g^{ab}$$

上述为模拟过程的完整描述。为了能使 $\mathscr{B}$ 成功地获得 Pr,需要分析不发生中断满足的条件。敌手可能产生的查询类型为对给定的身份 u, $F(u) = 0 (\mathrm{mod}\ \theta)$和 $F(u) \neq 0 (\mathrm{mod}\ \theta)$。如果 $F(u) = 0 (\mathrm{mod}\ \theta)$,则模拟终止。敌手可能给出的签名查询可表示为 $F(u_s) \neq 0 (\mathrm{mod}\ \theta)$, $F(u_s) = 0 (\mathrm{mod}\ \theta)$, $F(u_r) \neq 0 (\mathrm{mod}\ \theta)$, $F(u_s) = 0 (\mathrm{mod}\ \theta)$和 $F(u_r) = 0 (\mathrm{mod}\ \theta)$。

为了在模拟过程中避免被终止,有必要使生成查询的身份满足条件 $F(u_s) \neq 0 (\mathrm{mod}\ \theta)$,并且所有的签名信息$(u_s, m)$应该满足 $F(u_s) \neq 0 (\mathrm{mod}\ \theta)$。这样,尽管回答有些签名时可能会使 $F(u_s) = 0 (\mathrm{mod}\ \theta)$,但对于 $\mathscr{B}$ 攻击模拟终止的限制条件 Pr 的要求就更低了。

当 $\mathscr{B}$ 用任何身份为 $u (u \neq u^*, u^*$ 包括发送者和接收者的身份)查询时,不会使模拟过程终止的条件 Pr 满足 $F(u) \neq 0 (\mathrm{mod}\ \theta)$。设 $u_1, \cdots, u_{Q_I}$为生成查询或者签名查询中的值,并且不被包括在被挑战的身份中,则 $Q_I \leqslant Q_e + Q_s$。为 $1 \leqslant i \leqslant Q_I$ 定义事件 E_i', E_2, E_3 的形式如下:

$$E_i' : F(u_i) \neq 0 (\mathrm{mod}\ \theta)$$

$$E_2 : F(u^*) = 0 (\mathrm{mod}\ q)$$

$$E_3 : K(m''^*) = 0 (\mathrm{mod}\ q)$$

除了以上事件外还需要考虑事件 *HASHABORT*。

签名是在消息利用一个抗碰撞 Hash 函数生成的哈希值上进行的,因此有必要同时讨论不是由于 Hash 函数而终止的事件。设 $Adv_{TCR,H}^{Hash\text{-}tcr}(k)$ 表示敌手 $\mathscr{H}$ 利用 Kiltz 和 Galindo 两人的成果攻击目标抗碰撞 Hash 函数的优势,有

$$Pr[HASHABORT] \leqslant Adv_{TCR,H}^{Hash\text{-}tcr}(k) \tag{5}$$

如果敌手 $\mathscr{A}$ 找到一个碰撞值 Pr(至少为 $Pr[HASHABORT]$)就可以成功地完成对抗碰撞 Hash 函数的攻击。

在包括 $HASHABORT$ 事件的情况下,使 $\mathscr{B}$ 在模拟攻击过程中不会终止的 Pr 应该满足如下条件:

$$\begin{aligned}&(Pr[(E_1' \wedge E_2' \wedge E_3' \wedge \cdots \wedge E_{Q_I}') \wedge E_2]) \wedge \times Pr[E_3] \wedge Pr[\neg HASHABORT] \\ &= Pr\left[\bigwedge_{i=1}^{Q_I} E_i' \wedge E_2\right] \wedge \times Pr[E_3] \wedge Pr[\neg HASHABORT]\end{aligned} \tag{6}$$

在 $m(n+1) < q$ 的条件下,如果 $F(u) = 0(\mathrm{mod}\,\theta)$,则在[0,$n$]的范围内存在唯一 l 使得 $x' + \sum_{i \in U} x_i - \theta l = F(u) = 0(\mathrm{mod} q)$。由于 l,x'和 $\boldsymbol{x}$ 是随机选择的,通过概率的乘法运算可得:

$$Pr[E_2] = Pr[F(u^*) = 0(\mathrm{mod}\,q) \wedge F(u^*) = 0(\mathrm{mod}\,\theta)]$$

$$\begin{aligned}Pr[E_2] &= Pr[F(u^*) = 0(\mathrm{mod}\,\theta)] \cdot Pr[F(u^*) \\ &\quad = 0(\mathrm{mod}\,q) \mid F(u^*) = 0(\mathrm{mod}\,\theta)]\end{aligned}$$

$$Pr[E_2] = \frac{1}{\theta} \cdot \frac{1}{n+1}$$

$$Pr\left[\bigwedge_{i=1}^{Q_I} E_i' \wedge E_2\right] = Pr[E_2] \cdot Pr\left[\bigwedge_{i=1}^{Q_I} E_i' \mid E_2\right]$$

$$Pr\left[\bigwedge_{i=1}^{Q_I} E_i' \mid E_2\right] = 1 - Pr\left[\bigvee_{i=1}^{Q_I} \neg E_i' \mid E_2\right] = 1 - \sum_{i=1}^{Q_I} Pr[\neg E_i' \mid E_2]$$

如果对身份 u_1 和 u_2 的 $F()$为估计值,在 $F(u_1)$和 $F(u_2)$中的和是不同的,因为至少其中一个是随机选择的值。事件 $F(u_1) = 0(\mathrm{mod}\,\theta)$和 $F(u_2) = 0(\mathrm{mod}\,\theta)$是相互独立的。在特定的情况下对于任意的 i,E_i'和 E_2是相互独立的,又有 $Pr[\neg E_i' \mid E_2] = 1/\theta$,因此

$$Pr\left[\bigwedge_{i=1}^{Q_I} E_i' \wedge E_2\right] = \frac{1}{\theta(n+1)} \cdot \left(1 - \frac{Q_e + Q_s}{\theta}\right)$$

设 $\theta = 2(Q_e + Q_s)$,则

$$Pr\left[\bigwedge_{i=1}^{Q_I} E_i' \wedge E_2\right] \geqslant \frac{1}{4(n+1)(Q_e + Q_s)}$$

事件 E_3 中 Pr 的发生概率为 $1/\theta$。如果模拟过程没有终止,敌手 $\mathscr{A}$ 可以利用 Pr(至少为 ε)来完成一次可用的欺骗攻击。由(6)和(5),$\mathscr{B}$ 可以成功地解决 CDH 问题,至少成功的概率为

$$\frac{\varepsilon}{8(n+1)(Q_e + Q_s)^2}(1 - Adv_{TCR,H}^{Hash\text{-}tcr}(k))$$

$\mathscr{B}$ 的时间复杂度主要由求幂运算决定,然而对于较大的值 n,挑战者需要进

行 n 次乘法运算才能生成和进行 $3n+2$ 次签名查询;也就是说对于一个较大的值 n,生成查询运算需要的乘法的运行次数数量级为 $O(n)$。在生成查询运算的过程中求幂运算的复杂度为 $O(1)$,对于签名查询同样为 $O(1)$。敌手 $\mathcal{A}$ 需要的时间为 t,则 $\mathcal{B}$ 需要的时间为

$$t + O((Q_e \cdot n + Q_s \cdot n)\rho + (Q_e + Q_s)\tau)$$

方案 2 的安全性证明

方案 2 的证明继续使用方案 1 的证明流程。生成查询的过程同方案 1。签名查询的情况有以下三种情况:

情况 1:$F(u_s) \neq 0 (\bmod \theta)$。

情况 2:$F(u_s) = 0 (\bmod \theta)$,$K(m'') \neq 0 (\bmod \theta)$。

情况 3:$F(u_s) = 0 (\bmod \theta)$,$K(m'') = 0 (\bmod \theta)$。

对于情况 1,挑战者可以构建 u_s 的私钥,因此可以计算出一个签名。对于情况 2,挑战者可以构建 m''的私钥同时生成身份为 u_s 的签名。当在情况 3 的条件下模拟攻击过程意外终止时,将方案 2 过程降低为解决 CDH 问题的过程,方法如下:如果 $\mathcal{B}$ 没有终止,敌手将利用 Pr 返回 (u_s^*, m^*, c^*) 的值,其中 $c^* = (Z, A = g^t, B = g^{r_{u_s^*}^B})$,这也是一个对 (u_s^*, m^*) 的伪造。如果 $F(u_s^*) \neq 0 (\bmod q)$ 或者 $K(m''^*) = 0 (\bmod q)$,$\mathcal{B}$ 利用下面方法解决 CDH 问题:

$$\frac{Z}{A^{L(m''^*)m'} \cdot B^{J(u_s^*)}} = \frac{g_2^a \cdot g_{u_s^*}^{\tilde{r}_{u_s^*}} \cdot (g_{m''^*})^{m' \cdot t}}{(g_{m''^*})^{m't} \cdot g_{u_s^*}^{\tilde{r}_{u_s^*}}} = g^{ab}$$

参考文献

[1] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups, Lecture notes in computer science, 2003, Vol. 2567: 18-30.

[2] Boneh D, Franklin M. Identity based encryption from the weil pairing, Lecture notes in computer science, 2001, Vol. 2139: 213-229.

[3] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing, Lecture notes in computer science, 2001, Vol. 2248: 514-532.

[4] Desmedt Y, Quisquater J. Public-key systems based on the difficulty of tampering, Lecture notes in computer science, 1987, Vol. 263: 111-117.

[5] Feige U, Fiat A, Shamir A. Zero-knowledge proofs of identity, J. Cryptology, 1988, Vol. 1: 77-94.

[6] Fiat A, Shamir A. How to prove youself: practical solutions to identification and signature problems, Lecture notes in computer science, 1987, Vol. 263: 186-194.

[7] Galbraith S. Supersingular curves in cryptography, Lecture nores in computer sciences, 2001, Vol. 2248: 495-513.

[8] Menezes A. Elliptic curve public key cryptosystems, Kluwer Academic Publishers, 1993.

[9] Maurer U, Yacobi Y. Non-interective public-key cryptography, Lecture nores in computer sciences, 1992, Vol. 547: 498-507.

[10] Okamoto T, Pointcheval D. The gap-problems: a new class of problems for the security of cryptographic schemes, Lecture nores in computer sciences, 2001, Vol. 1992: 104-118.

[11] Pointcheval D, Stern J. Security proofs for signature schemes, Lecture notes in computer science, 1996, Vol. 1070: 387-398.

[12] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures, J. of cryptology, 2000, Vol. 13: 361-396.

[13] Shamir A. Identity-base cryptosystems and signature schemes, Lecture notes in computer science, 1985, Vol. 196: 47-53.

[14] Baek J, Safavi-Naini R, Susilo W. Efficient multi-receiver identity-based encryption and its application to broadcast encryption, Lecture notes in computer science, 2005, Vol. 3386: 380-397.

[15] Tanaka H. A realization scheme for the identity-based cryptosystem, Lecture nores in computer sciences, 1987, Vol. 293: 341-349.

[16] Tsuji S, Itoh T. An ID-based cryptosystem based on the discrete logarithm problem, IEEE Journal of selected areas in communications, 1989, Vol. 7, No. 4: 467-473.

[17] Yi X. An identity-based signature scheme from the weil pairing, Communications letters, 2003, Vol. 7: 76-78.

[18] Guillou L C, Quisquater J J. A paradoxical identity-based signature scheme resulting from zero-knowledge, Lecture notes in computer science, 1990, Vol. 196: 216-231.

[19] Lenstra A K. Selecting cryptographic key sizes, J. of cryptology, 2001, Vol. 14, No. 4: 255-293.

[20] Al-Riyami SS, Paterson K G. Certificateless public key cryptography, Lecture notes in computer science, 2003, Vol. 2894:452-473.

[21] Au M H, Huang Q, Liu J K. Willy Susilo, Duncan S. Wong and Guomin Yang, Traceable and retrievable identity-based encryption, Lecture notes in computer science, 2008, Vol. 5037: 94-110.

[22] Bwllare M, Boldyreva A, Desai A. Key-privacy in public-key encryption, Lecture notes in computer science, 2001, Vol. 2248: 566-582.

[23] Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes, J. of cryptology, 2009, Vol. 22, No. 1: 1-61.

[24] Bellare M, Palacio A. GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks, Lecture notes in computer science, 2002, Vol. 2442: 162-177.

[25] Boneh D, Boyen X. Short signatures without random oracles, Lecture notes in computer science, 2004, Vol. 3027: 56-73.

[26] Kiltza E, Galindo D. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles, Theoretical computer science, 2009, Vol. 410: 47-49.

[27] Chase M, Lysyanskaya A. On signatures of knowledge, Lecture notes in computer science, 2006, Vol. 4117: 78-96.

[28] Chen X. Zhang F, Kim K. New id-based group signature from pairings, Journal of electronics (CHINA), 2006, Vol. 23, No. 6: 892-900.

[29] Chow S S M. Removing escrow from identity-based encryption, Lecture notes in computer science, 2009, Vol. 5443: 256-276.

[30] Galindo D, Herranz J, Kiltz E. On the generic construction of identity-based signatures with additional properties, Lecture notes in computer science, 2006, Vol. 4284: 178-193.

[31] Gentry C. Certificate-based encryption and the certificate revocation problem, Lecture notes in computer science, 2003, Vol. 2656: 272-293.

[32] Gentry C, Silverberg A. Hierarchical ID-based cryptography, Lecture notes in computer science, 2002, Vol. 2501: 548-566.

[33] Girault M. Self-certified public keys, Lecture notes in computer science, 1991, Vol. 547: 490-497.

[34] Goyal V. Reducing trust in the PKG in identity based cryptosystems, Lecture notes in computer science, 2007, Vol. 4622: 430-447.

[35] Hu B C, Wong D S, Zhang Z. Key replacement attack against a generic construction of certificateless signature, Lecture notes in computer science, 2006, Vol. 4058: 235-246.

[36] Kang B G, Park J H, Hahn S G. A certificate-based signature scheme, Lecture notes in computer science, 2004, Vol. 2964: 99-111.

[37] Li J, Huang X, Mu Y, Susilo W. Certificate-based signature: Security model and efficient construction, Lecture notes in computer science, 2007, Vol. 4582: 110-125.

[38] Yuen T H, Susilo W, Mu Y. How to construct identity-based signatures without the key escrow problem, International journal of information Security, 2010, Vol. 9, No. 4: 297-311.

[39] Goldwasser S, Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal on computing, 1988, Vol. 17, issue. 2: 281-308.

[40] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption, Lecture Notes in computer science, 2002, Vol. 2332: 83-107.

[41] Boneh D, Boyen X. Efficient selective-ID secure identity-based encryption without random oracles, Lecture notes in computer science, 2004, Vol. 3027: 223-238.

[42] Boneh D, Boyen X. Secure identity based encryption without random oracles, Lecture notes in computer science, 2004, Vol. 3152: 197-206, 443-459.

[43] Bellare M, Boldyreva A, Palacio A. An uninstantiable randomoracle-model scheme for a hybrid-encryption problem, Lecture notes in computer science, 2004, Vol. 3027: 171-188.

[44] Barreto P S, Libert B, McCullagh N. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, Lecture notes in computer science, 2005, Vol. 3788: 515-532.

[45] Bellare M, Namprempre C, Neven G. Security proofs for identitybased identification and signature schemes, J. of cryptology, 2008, Vol. 22, No. 1: 1-61.

[46] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited, Journal of the ACM, 2004, Vol. 51, No. 4: 557-549.

[47] Cocks C. An identity based encryption scheme based on quadratic residues, Lecture notes in computer science, 2001, Vol. 2260: 360-363.

[48] Dodis Y, Katz J, Xu S. Strong key-insulated signature schemes, Lecture notes in computer science, 2003, Vol. 2567: 130-144.

[49] Hess F. Efficient identity based signature schemes based on pairings, Lecture notes in computer science, 2002, Vol. 2595: 310-324.

[50] Kiltz E, Mityagin A, Panjwani S. Append-only signatures, Lecture notes in computer science, 2005, Vol. 3580: 434-445.

[51] Chatterjee S, Sarkar P. Trading time for space: Towards an efficient IBE scheme with short (er) public parameters in the standard model, Lecture notes in computer science, 2006, Vol. 3935: 424-440.

[52] Waters B. Efficient identity-based encryption without random oracles, Lecture notes in computer science, 2005, Vol. 3494: 114-127.

[53] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model, Lecture notes in computer science, 2006, Vol. 4058: 207-222.

[54] Zhang F, Safavi-Naini R, Susilo W. An efficient signature scheme from bilinear pairings and its applications, Lecture notes in computer science, 2004, Vol. 2947: 277-290.

[55] Chow S S M, Yiu S M, Hui L C K. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity, Lecture notes in computer science, 2004, Vol. 2971: 352-369.

[56] Bellare M, Boldyreva A, Palacio A. An uninstantiable random oracle model scheme for a hybrid-encryption problem, Lecture notes in computer science, 2004, Vol. 3027: 171-188.

[57] Au M H, Liu J K, Yuen T H, Wong D S. ID - based ring signature scheme secure in the standard model, LNCS, 2006, Vol. 4266: 2-16.

[58] Cheon J H. Security analysis of the strong Diffie-Hellman problem, Lecture notes in computer science, 2006, Vol. 4004: 1-11.

[59] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, Lecture notes in computer science, 1998, Vol. 1462: 13-25.

[60] Paterson K G. ID-based signatures from pairings on elliptic curves, Electronics letters, 2002, Vol. 38, No. 18: 1025-1026.

[61] Narayan S, Parampalli U. EfFcient identity-based signatures in the standard model, IET information security, 2008, Vol. 2, No.4: 108-118.

[62] Paterson K G, Schuldt J C N. Efficient identity-based signatures secure in the standard model, Lecture notes in computer science, 2006, Vol. 4058: 207-222.

[63] Zhang M, Hu L, Li Q, Ju J. Weighted directed word graph. The proceedings of 16th annual symposium on combinatorial pattern matching (CPM 2005), Jeju Island, Korea, June 19-22, 2005. 156-167.

[64] Li Q, Feng Q, Hu L, Ju J. Fast two phrases PPM for IP traceback. The proceedings of 6th international conference on Parallel and distributed computing, applications and technologies (PDCAT 2005), Dalian, China, December 5-8, 2005:386-388.

[65] 林宇,于孟涛,王金玲,胡亮. 基于 IBE 和数字水印的电子印章解决方案,吉林大学学报(信息版),2007, Vol.25, No.4: 406-411.

[66] Hu L, Li H, Zhang Y, Wang Y, Yuan W. Identity-based short signature without randon oracles model. Proceedings of The ICIIA 2008 Conference, Guangzhou, China, 2008.11: 170-179.

第三章　基于身份的加密算法

3.1　基于身份加密算法介绍

自从 Shamir 于 1984 年提出基于身份加密算法的设计思想后，直到 2001 年，美国密码学家 Boneh 和 Franklin 利用椭圆曲线上的双线性映 Weil 配对设计出第一个真正实用的基于身份加密（IBE）方案。在他们开创性的工作之后，又有若干个在不依赖随机预言模型下被证明是安全的方案被提出。2003 年，Canetti 等人提出了一个被称为选择身份的弱 IBE 安全模型。在该模型中，敌手必须在全局参数产生之前声明它想要挑战的身份。同时，Canetti 还提供了一个在不依赖随机预言的选择身份模型下被证明是安全的方案。但是 Boneh 和 Franklin 方案及后来的一些方案在这种弱安全模型下被证明是不安全的。随后 Boneh 和 Boyen 提出了在“selective-ID”模型中更加实用的 IBE 系统，从而改善了 Canetti 的成果。此后不久 Boneh 和 Boyen 又提出了一个不依赖随机预言的完全安全方案，该方案中敌手可以适应性的选择要挑战的身份。2005 年，Waters 对该方案进行了简化，得到了一个优化执行效率的方案。2006 年，Gentry 分析了 Boneh 等人及 Waters 的 IBE 方案，指出 Boneh 和 Franklin 方案以后的所有 IBE 系统都利用了 Boneh 和 Franklin 的证明策略来证明其安全性，从而导致了其系统参数较长。通过分析和改进证明策略，Gentry 提出了一个系统参数较短的新 IBE 方案。

为了使读者全面了解基于身份加密算法，本章选取了 Boneh 和 Franklin 方案、Waters 方案及 Gentry 方案进行详细介绍，以充分展现 IBE 系统的特点。

3.2　基 础 模 型

3.2.1　基于身份的加密模型

基于身份的加密方案由四个随机算法组成：*Setup*，*Extract*，*Encrypt*，*Decrypt*。

Setup：输入一个安全参数 k 并返回系统参数 *params* 和主密钥。该系统参数包括一个有限的明文空间 M 的描述，和一个有限的密文空间 C。系统参数将被公开，而主密钥由私钥产生器（PKG）保留。

Extract:以主密钥,任意 $ID \in \{0,1\}^*$ 作为输入,并返回一个用户 *ID* 所对应的私钥 d。

Encrypt:以 *params*,*ID*,$m \in M$ 作为输入,返回密文 $c \in C$。

Decrypt:以密文 $c \in C$,私钥 d 及 *params* 作为输入,返回明文 $m \in M$。

这些算法必须满足标准一致性约束,即当私钥 d 由 Extract 算法生成时,$\forall m \in M$:$Decrypt(params,c,d) = m$,其中,$c = Encrypt(params,ID,m)$。

3.2.2 基于身份加密的安全模型

在选定一个身份攻击挑战下,如果在多项式时间内敌手没有一个不可忽略的优势赢得如下游戏挑战,IBE 系统具有选择密文安全性:

系统建立:挑战者运行系统建立过程算法,将 *params* 发送给敌手。

阶段 1:敌手自适应性的发出查询 $q_1,\cdots,q_m$,其中 q_i 可能为:

密钥生成查询$\langle ID_i\rangle$:挑战者在 ID_i 上运行 *KeyGen* 算法,并将产生的私钥发给敌手。

解密查询$\langle ID_i,c_i\rangle$:挑战者在身份 ID_i 上运行 *KeyGen* 算法,利用生成的私钥解密 c_i,然后将结果发给敌手。

挑战阶段:敌手提交两个明文 $m_0,m_1 \in M$ 和一个身份 *ID*。*ID* 必须在阶段 1 的密钥生成查询中没有出现过。挑战者选择一个随机比特 $b \in \{0,1\}$,设 $c = Encrypt(params,ID,m_b)$,将 c 发送给敌手作为其挑战密文。

阶段 2:除了敌手不可以请求 *ID* 的私钥和解密查询(*ID*,c)外,同阶段 1。

猜测阶段:敌手提交一个猜测 $b' \in \{0,1\}$。如果 $b = b'$则敌手成功,称敌手 $\mathcal{A}$ 在上述挑战过程中为一个 IND-ID-CCA 敌手。

定义 3.1 一个具有$(t,q_{ID},q_c,\varepsilon)$-IND-ID-CCA 安全的 IBE 系统为在 t 时间内所有 IND-ID-CCA 挑战者至多产生 q_{ID}次私钥查询,至多进行 q_c 次选择密文查询,至多有 ε 的概率取得挑战成功。

IND-ID-CCA 安全定义很简单,但是敌手不能进行解密查询。

定义 3.2 一个具有(t,q_{ID},ε)-IND-ID-CCA 安全的 IBE 系统是指其具有$(t,q_{ID},0,\varepsilon)$-IND-ID-CCA 的安全性。

可接受匿名访问:简单地说,一个 IBE 系统是匿名的,即一个敌手不能区分哪个 *ID* 对应的公钥用来产生了一个密文。可以通过以下修改使刚才的挑战具有匿名性:在挑战阶段,敌手输出两个没有在阶段 1 被查询的身份 ID_0,ID_1 和两个消息 m_0,m_1。挑战者选择两个随机比特 $a,b \in \{0,1\}$,利用 ID_a 加密 M_b,将结果密文 c 发送给敌手。阶段 2 除了敌手不能获得 ID_0,ID_1 的私钥和不能解密任何身份加密的密文 c 之外其余与阶段 1 相同。最后在猜测阶段,敌手猜测出两

个比特 a',b'。如果 $a=a',b=b'$ 则挑战成功。定义敌手在挑战过程中的优势为 $\left|Pr[a=a' \wedge b=b'] - \frac{1}{4}\right|$。

定义 3.3 一个具有 $(t,q_{ID},q_c,\varepsilon)$-ANON-IND-ID-CCA 安全性的 IBE 系统为在 t 时间内所有 ANON-IND-ID-CCA 挑战者至多产生 q_{ID} 次私钥查询，至多进行 q_c 次选择密文查询，按照上文改进的挑战过程至多有 ε 的概率取得挑战成功。

3.3 Boneh 和 Franklin 的 IBE 方案

3.3.1 方案描述

完整的加密方案由以下 *Setup*, *Extract*, *Encrypt* 和 *Decrypt* 四个随机算法组成。

Setup：给定参数 $k \in Z^+$，算法工作如下：

(1) 对于输入 k，生成素数 q，两个 q 阶群 G_1,G_2 和一个双线性映射 $e:G_1 \times G_1 \rightarrow G_2$。选择一个随机生成元 $P \in G_1$。

(2) 选择随机数 $s \in Z_q^*$，计算 $P_{pub}=sP$。

(3) 选择 Hash 函数 $H_1:\{0,1\}^* \rightarrow G_1^*$，$H_2:G_2 \rightarrow \{0,1\}^n$，$H_3:\{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*$，$H_4:\{0,1\}^n \rightarrow \{0,1\}^n$。这里安全分析将视 H_1,H_2 为随机预言。明文空间为 $M=\{0,1\}^n$，密文空间为 $C=G_1^* \times \{0,1\}^*$。公共系统参数 $params=\langle q,G_1,G_2,e,n,P,P_{pub},H_1,H_2,H_3,H_4\rangle$。主密钥 $s \in Z_q^*$。

Extract：对于给定的字符串 $ID \in \{0,1\}^*$，PKG 计算 $Q_{ID}=H_1(ID) \in G_1^*$，计算用户的私钥 $d_{ID}=sQ_{ID}$，其中 s 是 PKG 主密钥。

Encrypt：要在公钥 ID 下加密 $m \in M$，需做到以下几点：

(1) 计算 $Q_{ID}=H_1(ID) \in G_1^*$。

(2) 随机选择 $\sigma \in \{0,1\}^n$。

(3) 计算 $r=H_3(\sigma,m)$。

(4) 计算密文 $c=\langle rP,\sigma \oplus H_2(g_{ID}^r),m \oplus H_4(\sigma)\rangle$，其中 $g_{ID}=e(Q_{ID},P_{pub}) \in G_2^*$。

Decrypt：设 $c=\langle u,v,w\rangle$ 为使用公钥 ID 加密的密文。如果 $U \notin G_1^*$，则拒绝密文。为了用私钥 $d_{ID} \in G_1^*$ 解密密文 c，接收者进行如下操作：

(1) 计算 $V \oplus H_2(e(d_{ID},U))=\sigma$。

(2) 计算 $W \oplus H_4(\sigma)=m$。

(3) 计算 $r=H_3(\sigma,m)$ 并检测 $U=rP$ 是否成立。如果等式不成立，则拒

绝密文。

(4) 输出 m 作为 c 解密的明文。

3.3.2 安全性分析

下面的定理表明,假设 BDH 在由 G_1 群中是困难的,则前面介绍 IBE 方案是选择密文安全的(即 IND-ID-CCA)。

定理 3.1 设 Hash 函数 H_1, H_2, H_3, H_4 是随机预言。则 Boneh-Franklin 的 IBE 是一个选择密文安全的 IBE,(IND-ID-CCA)假设 BDH 在由 G_1 产生的群中是困难的。具体地说,假设有 IND-ID-CCA 的敌手 $\mathcal{A}$ 对于破解该方案有优势 $\varepsilon(k)$并且 $\mathcal{A}$ 最多的运行时间为 $t(k)$。假设 $\mathcal{A}$ 产生在最多 q_E 个提取查询,最多 q_D 个的解密查询,并在最多 $q_{H_2}, q_{H_3}, q_{H_4}$查询分别对应 Hash 函数 H_2, H_3, H_4。则对于 G_1 有一个 BDH 问题算法 $\mathcal{B}$ 的运行时间为 $t_1(k)$,其中:

$$Adv_{G,\mathcal{B}}(k) \geqslant 2FO_{adv}\left(\frac{\varepsilon(k)}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D\right)/q_{H_2}$$

$$t_1(k) \leqslant FO_{time}(t(k), q_{H_4}, q_{H_3})$$

其中,函数 FO_{time}和 FO_{adv}是在定理 3.2 定义的。

定理 3.1 的证明基于 Fujisaki 和 Okamoto 提出的定理。设 $BasicPub^{hy}$是采用 Fujisaki 和 Okamoto 转换的到 BasicPub 的结果。

定理 3.2(Fujisaki-Okamoto) 假设 IND-CCA 敌手 $\mathcal{A}$ 在挑战 $BasicPub^{hy}$时达到优势 $\varepsilon(k)$。$\mathcal{A}$ 的运行时间 $t(k)$,产生最多 q_D 个解密查询,使最多 q_{H_3}, q_{H_4}分别对应 Hash 函数 H_3, H_4 查询。然后对于 BasicPub 有一个 IND-CPA 敌手 $\mathcal{B}$,它具有运行时间 $t_1(k)$和优势 $\varepsilon_1(k)$其中:

$$\begin{aligned}\varepsilon_1(k) &\geqslant FO_{adv}(\varepsilon(k), q_{H_4}q_{H_3}, q_D)\\ &= \frac{1}{2(q_{H_4}+q_{H_3})}[(\varepsilon(k)+1)(1-2/q)^{q_D}-1]\\ t_1(k) &\leqslant FO_{time}(t(k), q_{H_4}, q_{H_3})\\ &= t(k)+O((q_{H_4}+q_{H_3})\cdot n)\end{aligned}$$

这里,q 是群 G_1, G_2 的大小,n 是 σ 的长度。

Fujisaki-Okamoto 证明了一个更强的结果:在定理 3.2 假设下 $BasicPub^{hy}$不是单向的加密方案。但这里对于定理 3.2 的目标结果是足够的。

为了证明定理 3.1,需要以下定理来在 Boneh-Franklin 的 IBE 方案上的 IND-ID-CCA 的选择密文攻击和 $BasicPub^{hy}$上的 IND-CCA 的密文选择攻击之间转换。

定理 3.3 设 $\mathcal{A}$ 是一个对于 Boneh-Franklin 的 IBE 方案具有优势 $\varepsilon(k)$的 IND-ID-CCA 敌手。假设 $\mathcal{A}$ 产生至多 $q_E>0$ 私钥提取的查询,最多 q_D 的解密查

询。然后有 IND-CCA 挑战者 $\mathcal{B}$ 对于 $BasicPub^{hy}$ 至少有优势 $\frac{\varepsilon(k)}{e(1+q_E+q_D)}$，运行时间 $O(time(\mathcal{A}))$。

证明：首先构造 IND-CCA 挑战者 $\mathcal{B}$，对于 $BasicPub^{hy}$ 使用 $\mathcal{A}$ 取得优势 $\varepsilon/e(1+q_E+q_D)$。挑战者和敌手之间的比赛以挑战者首先通过运行一个 $BasicPub^{hy}$ 的 keygen 算法生成随机公钥开始。其结果是公钥 $K_{pub}=\langle q,G_1,G_2,e,n,P,P_{pub},Q_{ID},H_2,H_3,H_4\rangle$ 并且私钥 $d_{ID}=sQ_{ID}$。算法将 K_{pub} 赋值给挑战者 $\mathcal{B}$。挑战者 $\mathcal{B}$ 在敌手 $\mathcal{A}$ 的帮助下向密钥 K_{pub} 发动 IND-CCA 攻击，$\mathcal{B}$ 与 $\mathcal{A}$ 交互如下：

Setup：挑战者 $\mathcal{B}$ 给敌手 $\mathcal{A}$ 系统参数 $\langle q,G_1,G_2,e,n,P,P_{pub},H_1,H_2\rangle$，这里 $\langle q,G_1,G_2,e,n,P,P_{pub},H_2\rangle$ 取自 K_{pub,H_1} 是由如下描述的 $\mathcal{B}$ 控制的随机预言：

H_1 查询：$\mathcal{A}$ 任何时间可以查询随机预言 H_1。为了回应这些查询，$\mathcal{B}$ 操作如下解释的元组 $\langle ID_j,Q_j,b_j,c_j\rangle$。把它记做 H_1^{list}，它初始为空。当 $\mathcal{A}$ 在点 ID_i 查询预言 H_1 的时候，$\mathcal{B}$ 响应如下：

（1）如果查询 ID_i 已经在 H_1^{list} 上的 $\langle ID_i,Q_i,b_i,c_i\rangle$ 中出现，则 $\mathcal{B}$ 以 $H_1(ID_i)=Q_i\in G_1^*$ 响应。

（2）否则，$\mathcal{B}$ 生成一个随机 $coin\in\{0,1\}$，所以 $Pr[coin=0]=\delta$ 对于一些 δ 将是待定的。

（3）$\mathcal{B}$ 选择随机 $b\in Z_q^*$。如果 $coin=0$，计算 $Q_i=bP\in G_1^*$；如果 $coin=1$，计算 $Q_i=bQ_{ID}\in G_1^*$。

（4）$\mathcal{B}$ 向 H_1^{list} 添加元组 $\langle ID_i,Q_i,b,coin\rangle$，使用 $H_1(ID_i)=Q_i$ 回应 $\mathcal{A}$。

请注意，无论中间节点 Q_i 在 G_1^* 中是否一致，它都要求当前视图中 $\mathcal{A}$ 是独立的。

Phase 1：解密查询。设 $\langle ID_i,c_i\rangle$，是一个由 $\mathcal{A}$ 发出的解密查询。设 $c_i=\langle U_i,V_i,W_i\rangle$。$\mathcal{B}$ 响应此查询如下：

（1）运行以上算法来响应 H_1 查询以获取 $Q_i\in G_1^*$，$H_1(ID_i)=Q_i$。设 $\langle ID_i,Q_i,b_i,coin_i\rangle$ 为 H_1^{list} 上的相应元组。

（2）假设 $coin_i=0$。在这种情况下，为对应的私钥查询运行算法用公钥 ID 获取私钥，然后用私钥响应解密查询。

（3）假设 $coin_i=1$，则 $Q_i=b_iQ_{ID}$。回顾 $U_i\in G_1$。令 $c_i'=\langle b_iU_i,V_i,W_i\rangle$。设 $d_i=sQ_i$ 是 Boneh-Franklin 的 IBE 方案对应 ID_i 的私钥。$BasicPub^{hy}$ 使用 d_{ID} 解密 c_i'，该方案使用 ID_i 解密 c_i。由此可得：

$$e(b_iU_i,d_{ID})=e(b_iU_i,sQ_{ID})=e(U_i,sb_iQ_{ID})=e(U_i,sQ_i)=e(U_i,d_i)$$

将解密查询 $\langle c_i'\rangle$ 传递给挑战者并且传递挑战者的响应返回到 $\mathcal{A}$。

Challenge：一旦 $\mathcal{A}$ 决定，第一阶段已经结束，它输出一个公钥 ID_{ch} 和两个消

息 m_0, m_1 其所希望受到挑战。$\mathscr{B}$ 回应如下：

(1) $\mathscr{B}$ 给出了挑战者 m_0, m_1 作为它希望受到挑战的信息，该挑战者使用 $BasicPub^{hy}$ 密文 $c=\langle U,V,W\rangle$ 响应，其中对于随机 $b\in\{0,1\}$，c 是 m_b 的加密。

(2) 接下来，$\mathscr{B}$ 运行对应的 H_1 查询的算法获得一个 $Q\in G_1^*$，使 $H_1(ID_{ch})=Q$。设 $\langle ID_{ch},Q,a,coin\rangle$ 为 H_1^{list} 上的元组。如果 $coin=0$，则 $\mathscr{B}$ 报告失败并终止，对 $BasicPub^{hy}$ 攻击失败。

(3) 如果 $coin=1$，则 $Q=aQ_{ID}$。回顾可知当 $c=\langle U,V,W\rangle$，可得 $U\in G_1^*$。

设 $c'=\langle a^{-1}U,V,W\rangle$，其中 a^{-1} 是 $\mathscr{B}$ 模 q 的逆。$\mathscr{B}$ 用挑战 c' 响应 $\mathscr{A}$。需要注意，c' 如同要求一样，在公钥 ID_{ch} 下是 m_b 的加密。

Phase 2：私钥查询。$\mathscr{B}$ 以在 *Phase* 1 中相同方式响应私钥提取查询。

Phase 3：解密查询。$\mathscr{B}$ 以在 *Phase* 1 中相同方式响应解密查询。但是，如果由此产生的解密查询转达给挑战者等同于挑战的密文 $c=\langle U,V,W\rangle$，则 $\mathscr{B}$ 报告失败并终止。对 $BasicPub^{hy}$ 攻击失败。

Guess：最终，$\mathscr{A}$ 输出 c 的猜想 c'。$\mathscr{B}$ 输出作为其 c' 的猜测 c。

Claim：如果 $\mathscr{B}$ 在模拟中不终止，则在模拟 $\mathscr{A}$ 看来它等同于在真正的攻击。此外，如果 $\mathscr{B}$ 不中止则概率超过了 $\mathscr{A}$，$\mathscr{B}$ 和挑战者使用的随机位的概率。

Proof of claim：由于每个反应是一致的并且独立地分布在 c_1^*，H_1 查询的响应如同真正的攻击。所有对于私钥提取查询和解密查询的反应都是有效的。最后，赋给 $\mathscr{A}$ 的挑战密文 c' 是对于一些随机 $b\in\{0,1\}$ 的 m_b 的一个加密。因此，由 $\mathscr{A}$ 的定义可得 $\left|Pr[b=b']-\frac{1}{2}\right|\geqslant\varepsilon$。

$\mathscr{B}$ 在模拟中是收敛的。该算法可以因为三种原因终止：(1) 在阶段 1 或 2，有一个来自 $\mathscr{A}$ 的坏的私钥查询；(2) $\mathscr{A}$ 选择一个坏的 ID_{ch} 受到挑战；(3) 第二阶段，一个来自 $\mathscr{A}$ 的坏的解密查询。这里定义三个相应的事件：

ε_1，$\mathscr{A}$ 在 1 或 2 阶段发行私钥查询时，导致 $\mathscr{B}$ 中止的事件。

ε_2，$\mathscr{A}$ 选择一个公钥 ID_{ch} 受到挑战时，导致 $\mathscr{B}$ 中止的事件。

ε_3，在模拟的第二阶段，$\mathscr{A}$ 发出一个解密查询解密：使解密查询传递给 $BasicPub^{hy}$ 的挑战者等于 c。已知使得 $c=\langle U,V,W\rangle$ 是来自 $BasicPub^{hy}$ 挑战者的挑战密文。

Claim：$Pr[\neg\varepsilon_1\wedge\varepsilon_2\wedge\neg\varepsilon_3]\geqslant\delta^{q_E+q_D}(1-\delta)$。

Proof of claim：通过引入由敌手产生的查询的最大数目响应 q_E+q_D 来证明 *claim*。设 $i=q_E+q_D$ 并且设 $\varepsilon^{0\cdots i}$ 是 $\mathscr{A}$ 发出最多 i 次查询后，$\varepsilon_1\vee\varepsilon_3$ 发生的事件。同样，设 ε^i 是 $\mathscr{A}$ 第 i 次查询后，$\varepsilon_1\vee\varepsilon_3$ 发生的事件。证明通过引入 i 使得 $Pr[\neg\varepsilon^{0\cdots i}\mid\neg\varepsilon_2]\geqslant\delta^i$。该 *claim* 表示如下：

$$Pr[\neg \varepsilon_1 \wedge \neg \varepsilon_2 \wedge \neg \varepsilon_3] = Pr[\neg \varepsilon_1 \wedge \neg \varepsilon_3 \mid \neg \varepsilon_2]$$
$$Pr[\neg \varepsilon_2] \geqslant Pr[\neg \varepsilon_1 \wedge \neg \varepsilon_3 \mid \neg \varepsilon_2](1-\delta)$$

对于 $i=0$ 的声称是可以忽略的，因为由定义，$Pr[\neg \varepsilon^{0\cdots 0}]=1$。现在 *claim* 中，$i-1$ 时假设成立。接着，

$$\begin{aligned} Pr[\neg \varepsilon^{0\cdots i} \mid \neg \varepsilon_2] &= Pr[\neg \varepsilon^{0\cdots i} \mid \neg \varepsilon^{0\cdots i-1} \wedge \neg \varepsilon_2] Pr[\neg \varepsilon^{0\cdots i-1} \mid \neg \varepsilon_2] \\ &= Pr[\neg \varepsilon^{i} \mid \neg \varepsilon^{0\cdots i-1} \wedge \neg \varepsilon_2] Pr[\neg \varepsilon^{0\cdots i-1} \mid \neg \varepsilon_2] \\ &\geqslant Pr[\neg \varepsilon^{i} \mid \neg \varepsilon^{0\cdots i-1} \wedge \neg \varepsilon_2] \delta^{i-1} \end{aligned}$$

因此，限定 $q_i = Pr[\neg \varepsilon^{i} \mid \neg \varepsilon^{0\cdots i-1} \vee \neg \varepsilon_2]$ 就足够了。换句话说，当界定了前 $i-1$ 次查询不会发生并且 ε_2 不会发生时，第 i 次查询就不会导致 ε^i 发生。考虑第 i 次查询通过 $\mathcal{A}$ 在模拟过程中发出的。查询可以是$\langle ID_i \rangle$的私钥查询或为$\langle ID_i, c_i \rangle$解密查询，其中 $c_i = \langle U_i, V_i, W_i \rangle$。如果查询是解密查询，则假设它需要发生在第二阶段，否则它在 ε_3 上没有效果。

设 $H_1(ID_i) = Q_i$，并设$\langle ID_i, Q_i, a_i, coin_i \rangle$是在 H_i^{list} 相应的元组。当 $coin_i = 0$ 时，查询不能导致事件 ε_1 的发生。同样，当 $coin_i = 0$ 时，查询不能引起事件 ε_3 的发生，因为在这种情况，$\mathcal{B}$ 不传递一个解密查询给 $BasicPub^{hy}$ 挑战者。用这些因素来约束 q_i，有四种情况需要考虑。在前三种情况下假设 ID_i 与 $\mathcal{A}$ 被挑战的公钥 ID_{ch} 是不相等的。

情况 1：第 i 次查询的 $\mathcal{A}$ 第一次发出含有 ID_i 的查询。在这种情况下 $Pr[coin_i = 0] = \delta$。因此，$q_i \geqslant \delta$。

情况 2：公钥 ID_i 在以前私钥的查询出现过。由于假设这一早期私钥查询没有造成的 $\varepsilon^{0\cdots i-1}$ 发生。已知 $coin_i = 0$，则有 $q_i = 1$。

情况 3：公钥 ID_i 的出现在以前的解密查询中。由于这一先前的假设解密查询没有导致事件的 $\varepsilon^{0\cdots i-1}$ 发生，则有 $coin_i = 0$ 或 $coin_i$ 对于 $\mathcal{A}$ 是独立的。无论哪种方式都可以得到 $q_i \geqslant \delta$。

情况 4：公钥 ID_i 等于 $\mathcal{A}$ 上正在受到挑战的公钥 ID_{ch}。通过定义可知，第 i 个查询不能是私钥查询。因此，它必须是一个解密查询$\langle ID_i, c_i \rangle$，此外，由于 ε_2 没有发生，当 $coin_i = 1$，所以 $\mathcal{B}$ 将传递解密查询 c_i'给 $BasicPub^{hy}$ 挑战者。设 c'为给予 $\mathcal{A}$ 的挑战是密文。由定义可知，$c_i \neq c'$。由此可见，$c_i' \neq c$，因此该查询不能使 ε_3 的事件发生。因此，在这种情况下，$q_i = 1$。

总之，无论第 i 次查询是什么，都有 $q_i = 1$。因此，有如下要求 $Pr[\neg \varepsilon^{0\cdots i} \mid \neg \varepsilon_2] \geqslant \delta^i$。现在 *claim* 进行如下设置 $i = q_E + q_D$。

为了完成对定理 3.3 证明，它保持了对 δ 选择优化。由于 $Pr[\neg \varepsilon_1 \mid \wedge \neg \varepsilon_2 \wedge \neg \varepsilon_3] \geqslant \delta^{q_E+q_D}(1-\delta)$ 的成功概率最大化为 $\delta_{opt} = 1 - 1/(q_E + q_D + 1)$，使 δ_{opt} 成

立的概率至少保持为$\frac{1}{e(1+q_E+q_D)}$。这表明，$\mathcal{B}$要求优势至少为$=\varepsilon/e(1+q_E+q_D)$。

证明定理 3.1 可通过定理 3.3，FullIdent 上的 IND-ID-CCA 的敌手等同于 $BasicPub^{hy}$上的 IND-CCA 敌手。通过定理 3.2，$BasicPub^{hy}$上的 IND-CCA 敌手等同于 *BasicPub* 上的 IND-CPA 敌手。

3.4 Waters 的 IBE 方案

3.4.1 方案描述

令 G 是 p 阶的群，其中 p 为素数，在 G 中存在一个到 G_1 的高效可计算的双线性映射。此外，令 $e:G\times G\rightarrow G_1$ 表示该双线性映射，$g\in G$ 是对应的生成元。群的大小是由安全参数决定的。身份用长度为 n 的比特位串来表示，n 是一个与 p 无关的独立参数。也可以令身份是任意比特长的串，而 n 是一个抗碰撞 Hash 函数 $H:\{0,1\}^*\rightarrow\{0,1\}^n$ 的输出长度。Waters 的 IBE 方案如下：

Setup：系统参数的产生过程如下。随机选择 $\alpha\in Z_p$。选择一个随机的生成元 $g\in G$，计算 $g_1=g^\alpha$，并在 G 中随机选择 g_2。此外，PKG 选择一个随机值 $u'\in G$ 和一个随机的长度为 n 的向量 $\boldsymbol{u}=(u_i)$，它的元素都是从 G 中随机选择的。公布公共参数 g,g_1,g_2,u'和 $\boldsymbol{u}$。保留主私钥 g_2^α。

KeyGen：令 v 是一个 n 比特的字符串，用它来表示身份，v_i 表示 v 的第 i 个比特，$V\subseteq\{1,\cdots,n\}$ 是满足 $v_i=1$ 的所有 i 的集合。（也就是 V 是比特串中为 1 的位的索引的集合）。身份 v 的私钥产生如下：首先，选择一个随机值 $r\in Z_p$，那么私钥构建如下：

$$d_v=\left(g_2^\alpha\left(u'\coprod_{i\in V}u_i\right)^r,g^r\right)$$

Encrypt：使用身份对消息 $m\in G_1$ 按如下方法进行加密。随机选择值 $t\in Z_p$。那么密文构建如下：

$$c=\left(e(g_1,g_2)^t m,g^t,\left(u'\coprod_{i\in V}u_i\right)^t,g\right)$$

Decrypt：令 $c=(C_1,C_2,C_3)$是身份 v 下的对消息 m 的有效的加密，那么 c 可以使用 $d_v=(d_1,d_2)$解密如下：

$$C_1\frac{e(d_2,C_3)}{e(d_1,C_2)}=(e(g_1,g_2)^t m)\frac{e\left(g^r,\left(u'\prod_{i\in V}u_i\right)^t\right)}{e\left(g_2{}^\alpha\left(u'\prod_{i\in V}u_i\right)^r,g^t\right)}$$

$$= (e(g_1,g_2)^t m)\frac{e\left(g,\left(u'\prod_{i\in V}u_i\right)^{rt}\right)}{e(g_1,g_2)^{te}\left(\left(u'\prod_{i\in V}u_i\right)^{rt},g\right)} = m$$

如果 $e(g_1,g_2)$ 被缓存了，那么加密需要 G 中平均 $n/2$（至多 n）的群操作，G 中两个指数运算，G_1 中一个指数运算，和 G_1 中一个群操作。解密需要两个双线性映射计算，G_1 中一个群操作和一个逆运算。

3.4.2 安全性分析

定理 3.4 如果判定性 $\left(t+O(\varepsilon^{-2}\ln(\varepsilon^{-1})\lambda^{-1}\ln(\lambda^{-1})),\frac{\varepsilon}{32(n+1)q}\right)$ BDH 假设成立，其中 $\lambda=\frac{1}{8(n+1)q}$，上面的 IBE 方案是 (t,q,ε) 安全的。

证明：假设存在一个 (t,q,ε) 敌手 $\mathcal{A}$。构建一个挑战者 $\mathcal{B}$ 来进行判定性 BDH 游戏攻击。挑战者接收 BDH 挑战攻击 $(g,A=g^a,B=g^b,C=g^c,Z)$，无论挑战攻击是不是 BDH 元组都输出一个猜测值 β'。挑战者执行下面的步骤。

模拟的过程描述如下：

Setup：挑战者首先设置一个整数，$\theta=4q$，并从 0 至 n 之间均匀地随机选择一个整数 k。然后挑战者选择一个随机的长度为 n 的向量，$\boldsymbol{x}=(x_i)$，其中 $\boldsymbol{x}$ 的元素是从整数 0 至 $n-1$ 之间随机选择的，值 x' 是从 0 至 $\theta-1$ 之间随机选择的。令 X^* 表示对 $(x',\boldsymbol{x})$。此外，挑战者还选择一个随机数 $y'\in Z_p$ 和一个长度为 n 的向量 $\boldsymbol{y}=(y_i)$，其中 $\boldsymbol{y}$ 的元素是从 Z_p 中随机选取的。这些值都是由挑战者内部保存的。

同样，对于身份 v，令 $V\subseteq\{1,\cdots,n\}$ 是所有 $v_i=1$ 的 i 的集合。为了简化分析需要定义三个函数：$F(v)=(p-\theta k)+x'+\sum_{i\in V}x_i$，$J(v)=y'+\sum_{i\in V}y_i$ 和二元函数 $K(v)=\begin{cases}0, & \text{if } x'+\sum_{i\in V}x_i\equiv 0(\bmod\theta)\\ 1, & \text{otherwise}\end{cases}$。

挑战者赋值 $g_1=A$ 和 $g_2=B$，然后赋值公共参数 $u'=g_2^{p-k\theta+x'}g^{y'}$ 和 $u_i=g_2^{x_i}g^{y_i}$。从敌手的角度来看公共参数的分布与真实的构建是等同的。

Phase 1：敌手 $\mathcal{A}$ 将提交私钥查询。假定敌手提交一个对身份 v 的查询。如果 $K(v)=0$，那么挑战者终止并随机选择值 β' 作为他对挑战者的 β 的猜测结果。否则，挑战者选择一个随机数 $r\in Z_p$。挑战者构建私钥 d 如下：

$$d=(d_0,d_1)=\left(g_1^{\frac{-J(v)}{F(v)}}\left(u'\prod_{i\in V}u_i\right)^r,g_1^{\frac{-1}{F(v)}}g^r\right)$$

令 $\tilde{r}=r-\frac{a}{F(v)}$，于是有

$$
\begin{aligned}
d_0 &= g_1^{\frac{-J(v)}{F(v)}}\left(u'\prod\nolimits_{i\in V}u_i\right)^r \\
&= g_1^{\frac{-J(v)}{F(v)}}\left(g_2^{F(v)}g^{J(v)}\right)^r \\
&= g_2^{a}\left(g_2^{F(v)}g^{J(v)}\right)^{-\frac{a}{F(v)}}\left(g_2^{F(v)}g^{J(v)}\right)^r \\
&= g_2^{a}\left(u'\prod\nolimits_{i\in V}u_i\right)^{r-\frac{a}{F(v)}} \\
&= g_2^{a}\left(u'\prod\nolimits_{i\in V}u_i\right)^{\tilde{r}}
\end{aligned}
$$

此外，有 $d_1 = g_1^{\frac{-1}{F(v)}}g^r = g^{r-\frac{a}{F(v)}} = g^{\tilde{r}}$。

当且仅当 $F(v)\neq 0(\mathrm{mod}\,p)$ 时，这个挑战者能够执行这个运算。为了简化分析，在充分条件 $K(v)\neq 0$ 下，挑战者只是继续（而不是终止）。（如果有 $K(v)\neq 0$，这就意味着 $F(v)\neq 0(\mathrm{mod}\,p)$，因为对于任何合理的 p，n 和 θ 的值，可以假定 $p > n\cdot\theta$。）

Challenge：敌手接下来将提交两条消息 $m_0, m_1 \in G_1$ 和身份 v^*。如果 $x' + \sum_{i\in V^*} x_i \neq k\cdot\theta$，那么挑战者将终止，并提交一个 β' 的随机猜测值。否则 $F(v^*)\equiv 0(\mathrm{mod}\,p)$，那么挑战者抛出硬币 γ，并构建密文 $t = (Zm_\gamma, c, c^{J(v^*)})$。

假定挑战者被给定一个 BDH 元组即 $Z = e(g,g)^{abc}$。那么 $t = (e(g,g)^{abc}m_\gamma, g^c, c^{cJ(v^*)}) = (e(g_1,g_2)^c m_\gamma, g^c, (u'\prod_{i\in V^*}u_i)^c)$。可以看到 t 是消息 m_γ 的有效加密。否则，有 Z 是 G 中的一个随机元素。那么这种情况密文就不会给出挑战者选择的 γ 的任何消息。

Phase 2：挑战者重复 *Phase* 1 中使用的方法。

Guess：最后，敌手 $\mathcal{A}$ 输出对 γ 的猜测值 γ'。

Artificial Abort：此时模拟还是无法使用敌手的输出结果。敌手成功的概率可以和挑战者需要终止的概率相关联。这个结论源于这样的事实：两个不同的 q 次私钥查询集合会以不同的概率引起挑战者终止。在最坏的情况下，在模拟环境中，可能会担心 $Pr[\gamma=\gamma' \mid \neg\, abort] - \frac{1}{2} = 0$（或者是一个可以忽略的值），即使对于一些不可忽略的 ε 也有 $Pr[\gamma=\gamma'] - \frac{1}{2} = \varepsilon$。

根据上面提到的内容可知，挑战者强制将由于敌手寻问可能导致模拟终止的查询集合的概率设定为 $(1-\lambda)$，其中 $(1-\lambda)$ 是此阶段之前引起挑战者终止私钥查询的集合的概率下界。

令 $\boldsymbol{v} = \{v_1,\cdots,v_q\}$ 表示 *Phase* 1 和 *Phase* 2 中产生的私钥查询，v^* 表示挑战攻击身份，$V^*\subseteq\{1,\cdots,n\}$ 是所有满足 $v_i^* = 1$ 的 i 的集合。首先定义函数 $\tau(X',\boldsymbol{v},$

v^*),其中 X'是模拟值 $x', x_1, \cdots, x_n$ 的集合:

$$\tau(X', \boldsymbol{v}, v^*) = \begin{cases} 0, & \text{if}(\wedge_{i=1}^{q} K(v_i) = 1) \wedge x' + \sum_{i \in V^*} x_i = k \cdot \theta \\ 1, & \text{otherwise} \end{cases}$$

如果对于一个给定的模拟环境值 X',私钥和攻击查询挑战问询 $\boldsymbol{v}, v^*$ 并没有导致挑战者终止,那么函数 $\tau(X', \boldsymbol{v}, v^*)$ 的值为 0。这时可以根据给定的查询集合 $\boldsymbol{v}$ 和 v^* 的模拟环境变量值来分析概率 $\eta = Pr_{X'}[\tau(X', \boldsymbol{v}, v^*) = 0]$。

挑战者通过选择随机的 X'对概率 η 采样 $O(\varepsilon^{-2}\ln(\varepsilon^{-1})\lambda^{-1}\ln(\lambda^{-1}))$次,并通过运行 $\tau(X', \boldsymbol{v}, v^*)$来估计值 η'。值得注意的是采样并不需要敌手运行。令 $\lambda = \frac{1}{8nq}$是挑战者对任何查询集合都没终止的概率的下界。(下面会说明如何计算 λ。)如果 $\eta' \geqslant \lambda$,那么挑战者就会以$\frac{\eta' - \lambda}{\eta'}$的概率终止(而不是以$\frac{\lambda}{\eta'}$的概率终止),并且接受一个随机猜测值 β'。否则,挑战者就不会终止。

如果挑战者此时没有终止,它就会检查敌手的猜测值是否 $\gamma' = \gamma$。如果 $\gamma' = \gamma$,那么挑战者输出一个猜测值 $\beta' = 1$,否则输出 $\beta' = 0$。

这些就是对挑战者的描述。

对挑战者直接分析比较困难,因为它可能会在所有的查询产生之前终止。所以描述第二个模拟环境来用它推理第一个模拟环境的输出分布。

Setup:在构建中挑战者选择秘密密钥 g_2^{α},然后如第一个模拟环境一样选择 $X^*, \boldsymbol{y}$ 并以相同的方式产生 u', U。然后运行敌手。

Phase 1:挑战者如在构建中一样使用主密钥来响应私钥查询,这样所有的查询都可以得到应答。

Challenge:挑战者接收到挑战消息 m_0, m_1。第二个挑战者将会翻转两个硬币 β 和 γ。如果 $\beta = 0$,那么挑战者加密一个随机消息,如果 $\beta = 1$,它加密消息 m_γ。

Phase 2 和 *Phase* 1 相同。

Guess:挑战者接收到来自敌手的猜测值 γ'。此时挑战者已经看过私钥查询和挑战查询$(\boldsymbol{v}, v^*)$。挑战者计算函数 $\tau(X', \boldsymbol{v}, v^*)$,如果计算值为 1 就终止,并输出 β'的随机猜测值。

Artificial Abort:最后一步的做法严格说来和第一个模拟环境一样。到这里描述结束。

首先用下面的 *Claim* 使两个挑战者的概率相等。

Claim 1:概率 $Pr[\beta' = \beta]$在第一个和第二模拟环境中是一样的。

证明:第二个模拟环境完全地运行敌手并接收所有敌手的查询。在 *Guess* 阶段检查如果 $\tau(X', \boldsymbol{v}, v^*) = 1$ 就终止。这个检查决定了是否存在一个时间点。

在这个时间点第一个挑战者需要在模拟期间终止并接收一个随机猜测。

如果存在这个点，那么第二个挑战者终止并接收一个随机猜测。此外，所有的公共参数，私钥查询，和挑战密文在可能的终止之前具有相同的分布，并且在人工终止阶段也是等同的。因此输出分布也是一样的。

Claim 2：模拟环境在猜测阶段之前没有终止的概率至少是 $\lambda = \frac{1}{8(n+1)q}$。

证明：计算对于所有的(v, v^*)的 $Pr_{X'}[\tau(X', v, v^*) = 0]$的下界 λ。为了不失通用性，假设敌手总是产生最大数量 q 次的查询。对于任何的 q 次查询的集合 $v_1, \cdots, v_q$ 和挑战身份 v^*，有 $Pr[\neg\, abort] = Pr[(\bigwedge_{i=1}^{q} K(v_i) = 1) \wedge \sum_{i \in V^*} x_i = k\theta]$。然后就可以定出没有终止的概率的下界如下：

$$Pr\left[\left(\bigwedge_{i=1}^{q} K(v_i) = 1\right) \wedge \sum_{i \in V^*} x_i = k\theta\right] \tag{1}$$

$$= \left(1 - Pr\left[\bigvee_{i=1}^{q} K(v_i) = 0\right]\right) Pr\left[\sum_{i \in V^*} x_i = k\theta \mid \bigwedge_{i=1}^{q} K(v_i) = 1\right] \tag{2}$$

$$\geqslant \left(1 - \sum_{i=1}^{q} Pr[K(v_i) = 0]\right) Pr\left[\sum_{i \in V^*} x_i = k\theta \mid \bigwedge_{i=1}^{q} K(v_i) = 1\right] \tag{3}$$

$$= \left(1 - \frac{q}{\theta}\right) Pr\left[\sum_{i \in V^*} x_i = k\theta \mid \bigwedge_{i=1}^{q} K(v_i) = 1\right] \tag{4}$$

$$= \frac{1}{n+1}\left(1 - \frac{q}{\theta}\right) Pr\left[K(v^*) = 0 \mid \bigwedge_{i=1}^{q} K(v_i) = 1\right] \tag{5}$$

$$= \frac{1}{n+1}\left(1 - \frac{q}{\theta}\right) \frac{Pr[K(v^*) = 0]}{Pr[\wedge_{i=1}^{q} K(v_i) = 1]} Pr\left[\bigwedge_{i=1}^{q} K(v_i) = 1 \mid K(v^*) = 0\right] \tag{6}$$

$$\geqslant \frac{1}{(n+1)\theta}\left(1 - \frac{q}{\theta}\right) Pr\left[\bigwedge_{i=1}^{q} K(v_i) = 1 \mid K(v^*) = 0\right] \tag{7}$$

$$= \frac{1}{(n+1)\theta}\left(1 - \frac{q}{\theta}\right)\left(1 - Pr\left[\bigvee_{i=1}^{q} K(v_i) = 0 \mid K(v^*) = 0\right]\right) \tag{8}$$

$$\geqslant \frac{1}{(n+1)\theta}\left(1 - \frac{q}{\theta}\right)\left(1 - \sum_{i=1}^{q} Pr\left[K(v_i) = 0 \mid K(v^*) = 0\right]\right) \tag{9}$$

$$= \frac{1}{(n+1)\theta}\left(1 - \frac{q}{\theta}\right)^2 \tag{10}$$

$$\geqslant \frac{1}{(n+1)\theta}\left(1 - 2\frac{q}{\theta}\right) \tag{11}$$

等式(4)和(7)来自于事实，即对于任何查询 v 有 $Pr[K(v) = 0] = \frac{1}{\theta}$。等式(5)中的因式$\frac{1}{n+1}$来自于挑战者接收对 k 的猜测值。等式(10)是源于对任何一对

不同的查询 v,v'的两两独立的概率 $K(v)=0,K(v')=0$。概率是两两独立的,因为总和 $x'+\sum_{i\in V}x_i(\mathrm{mod}\theta)$ 与 $x'+\sum_{i\in V'}x_i(\mathrm{mod}\theta)$ 至少有一个随机数 x_j 是不同的。

可以通过使 $\theta=4q$ 来最优化最后一个等式,其中 q 是查询的最大数。(如果敌手进行较少的,那么没有终止的概率就只能会更大。)解决了这个问题可以得出一个下界 $\lambda=\frac{1}{8(n+1)q}$。

现在可以计算 P_{BDH}和 R_{BDH}。R_{BDH}的分布就是 1/2。当挑战者被给定一个随机元素作为元组中的最后一项,挑战者或者终止(并有 1/2 的概率猜测 $\beta'=1$),或者当敌手准确地猜测出 γ 时它也猜测 $\beta'=1$。不过,在这个情况中 γ 对敌手来说是完全隐藏的,所以敌手正确的概率是 1/2。

P_{BDH}的计算稍微有点复杂。在第二个模拟环境中敌手对模拟环境的看法和真实游戏是一样的。需要知道猜测 $\beta'=1$ 的概率。

将事件分为终止和不终止两种情况,那么 $Pr[\beta'=1]$ 就是 $Pr[\beta'=1\mid abort]Pr[abort]$与 $Pr[\beta'=1\mid\neg abort]Pr[\neg abort]$两者的和。需要强调的是 $Pr[\beta'=1\mid abort]=\frac{1}{2}$以及当敌手正确地猜测出 $\gamma'=\gamma$ 而挑战者没有终止时 $\beta'=1$。则有 $P_{\mathrm{BDH}}=\frac{1}{2}+\frac{1}{2}(Pr[\neg abort\mid\gamma'=\gamma]Pr[\gamma'=\gamma]-Pr[\neg abort\mid\gamma'\neq\gamma]Pr[\gamma'\neq\gamma])$。根据假定,它是与 $\frac{1}{2}+\frac{1}{2}\left(Pr[\neg abort\mid\gamma'=\gamma]\left(\frac{1}{2}+\varepsilon\right)-Pr[\neg abort\mid\gamma'\neq\gamma]\left(\frac{1}{2}-\varepsilon\right)\right.$相等的。接下来还要做的就是定出在模拟环境中没有终止的概率的下界和上界。

Claim 3:如果挑战者在计算估计值 η'时进行了 $O(\varepsilon^{-2}\ln(\varepsilon^{-1})\lambda^{-1}\ln(\lambda^{-1}))$次采样,那么$\left(\frac{1}{2}+\varepsilon\right)Pr[\neg abort\mid\gamma'=\gamma]-\left(\frac{1}{2}-\varepsilon\right)Pr[\neg abort\mid\gamma'=\gamma]\geqslant\frac{3}{2}\lambda\varepsilon$。

证明略。

根据上面的 *Claim* 3,有 $P_{\mathrm{BDH}}\geqslant\frac{1}{2}+\frac{3}{4}\lambda\varepsilon$。于是$\frac{1}{2}(P_{\mathrm{BDH}}-R_{\mathrm{BDH}})\geqslant\frac{3}{4}\lambda\varepsilon\geqslant\frac{\varepsilon}{32(n+1)q}$。

注意:对于挑战者如果存在一种方法能够高效地计算终止概率 η,对于给定的查询集合(与采样的相反),那么就能在简化分析同时显著地改善收敛的时间。

3.5 Gentry 的 IBE 方案

Gentry 的 IBE 方案是一个基于随机预言模型的，在简化版的 $(q_{ID}+2)$-ABDHE 假设成立的前提下，具有 ANON-IND-ID-CCA 安全性的高效 IBE 系统。

3.5.1 构建过程

设 G, G_T 阶为 p 的群，设 $e: G \times G \rightarrow G_T$ 是双线性映射。IBE 系统按照如下过程工作：

Setup：PKG 随机选择生成元 $g, h_1, h_2, h_3 \in G$，随机选择 $\alpha \in Z_p$。设 $g_1 = g^{\alpha} \in G$。选择一个单向的 Hash 函数 H，公共参数 *params*，以及私钥 *master-key* 如下：$params = (g_1, g_2, h_1, h_2, h_3, H)$，$master\text{-}key = \alpha$。

KeyGen：PKG 产生随机值 $r_{ID,i} \in Z_p$ 其中 $i \in \{1,2,3\}$ 来生成身份 $ID \in Z_p$ 的私钥，输出私钥如下：$d_{ID} = \{(r_{ID,i}, h_{ID,i}): i \in \{1,2,3\}\}$ 其中 $h_{ID,i} = (h_i g^{-r_{ID,i}})^{1/(\alpha - ID)}$。若 $ID = \alpha$ 则 PKG 终止。要求 PKG 对于 ID 总是使用同样的随机值 $\{r_{ID,i}\}$。

Encrypt：使用身份 $ID \in Z_p$ 来加密 $m \in G_T$，发送者产生随机 $s \in Z_p$ 并且发送密文 $c = (g_1^s g^{-s \cdot ID}, e(g,g)^s, m \cdot e(g,h)^{-s}, e(g,h_2)^s e(g,h_3)^{s\beta})$。

上式中，对于 $c = (u,v,w,y)$，设 $\beta = H(u,v,w)$，加密不要求任意配对计算，$e(g,g)$ 和 $\{e(g,h_1)\}$ 已经被预先计算出来。或者 $e(g,g)$ 和 $\{e(g,h_1)\}$ 被包含在系统参数中，其中 h_i 可以被忽略。

Decrypt：利用身份 ID 解密密文 $c = (u,v,w,y)$，接收者计算 $\beta = H(u,v,w)$，并测试 $y = e(u, h_{ID,2} h_{ID,3}^{\beta}) v^{r_{ID,2} + r_{ID,3}\beta}$，如果等式不成立，则返回错误提示，如果等式成立，接收者输出 $m = w \cdot e(u, h_{ID,1}) v^{r_{ID,1}}$。

正确性：

$$
\begin{aligned}
& e(u, h_{ID,2} h_{ID,3}) v^{r_{ID,2} + r_{ID,3}\beta} \\
&= e(g^{s(\alpha - ID)}, (h_2 h_3^{\beta})^{1/(\alpha - ID)} g^{-(r_{ID,2} + r_{ID,3}\beta)/(\alpha - ID)}) e(g,g)^{s(r_{ID,2} + r_{ID,3}\beta)} \\
&= e(g^{s(\alpha - ID)}, (h_2 h_3^{\beta})^{1/(\alpha - ID)}) \\
&= e(g,h_2)^s e(g,h_3)^{s\beta}
\end{aligned}
$$

因此，验证结果正确，具有 ANON-IND-ID-CPA 安全性的方案

$$e(u, h_{ID,1}) v^{r_{ID,1}} = e(g^{s(\alpha - ID)}, h_1^{1/(\alpha - ID)} g^{-r_{ID,1}/(\alpha - ID)}) e(g,g)^{s r_{ID,1}} = e(g,h_1)^s$$

符合要求。

3.5.2 安全性

在简化的决定性$(q_{ID}+2)$-ABDHE 假设条件下证明上文的 IBE 系统具有 ANON-IND-ID-CCA 安全性。

定理 3.5 设$q=q_{ID}+2$,假设(G,G_T,e)满足简化的决定性(t,ε,q)-ABDHE 假设,从而上述 IBE 系统当$t'=t-O(t_{exp}\cdot q^2)$和$\varepsilon'=\varepsilon+4q_C/p$,其中$t_{exp}$是在$G$中计算幂值所需要的时间,是具有$(t',\varepsilon',q_{ID})$-ANON-IND-ID-CPA 安全性的。

证明:设$\mathcal{A}$是一个具有$(t',\varepsilon',q_{ID},q_c)$概率攻破上文中具有 ANON-IND-ID-CCA 安全性系统的敌手。设计一个算法$\mathcal{B}$,用来解决简化的决定性q-ABDHE 问题,具体如下:$\mathcal{B}$将随机简化的决定性q-ABDHE 攻击$(g',g'_{q+2},g,g_1,\cdots,g_q,Z)$,其中$Z$或者为$e(g_{q+1},g')$或者为$G_T$中的随机元素,作为输入。算法$\mathcal{B}$使用方法如下:

系统建立:$\mathcal{B}$产生一个q阶的随机多项式$f_i(x)\in Z_p[x],i\in\{1,2,3\}$。设$h_i=g^{f_i(\alpha)}$,从$(g,g_1,\cdots,g_q)$中计算$h$。将公钥$(g,g_1,h_1,h_2,h_3)$发送给$\mathcal{A}$。由于$g$,$\alpha$和$f_i(x)$是随机一致选择出来的,则$h_1,h_2,h_3$是一致的随机数并且公钥与实际构建中有同样的分布。

阶段 1:$\mathcal{A}$产生密钥生成查询。$\mathcal{B}$按如下方式回复对于身份$ID\in Z_p$的查询。如果$ID=\alpha$,$\mathcal{B}$立即使用α来解决简化的决定性q-ABDHE 问题。或者产生一对$(r_{ID,1},h_{ID,1})$使得$h_{ID,1}=(h_1g^{-r_{ID,1}})^{1/(\alpha+ID)}$,$\mathcal{B}$设置$r_{ID,1}=f_1(ID)$并按证明定理 3.4 的过程计算$h_{ID,1}$。同样的方法计算私钥的剩余部分。这样为身份$ID$产生的私钥是有效的。

$\mathcal{A}$也产生解密查询,为了回复一个(ID,c)的解密查询,$\mathcal{B}$按上述过程产生ID的私钥。利用这个私钥和一般的解密算法就可以解密密文c。

攻击过程:$\mathcal{A}$输出身份ID_0,ID_1以及消息m_0,m_1。如果$\alpha\in\{ID_0,ID_1\}$,$\mathcal{B}$立即使用α来解决简化的决定性q-ABDHE 问题。或者像以前一样,$\mathcal{B}$产生比特$a,b\in\{0,1\}$。在计算ID_a的私钥$\{(r_{ID,i},h_{ID,i}):i\in\{1,2,3\}\}$后,再像以前一样计算$(u,v,w)$,其中利用$(r_{ID_a,1},h_{ID_a,1})$的部分密钥计算出$w$。设$\beta=H(u,v,w)$,$\mathcal{B}$设$y=e(u,h_{ID,2}h_{ID,3}^{\beta})v^{r_{ID,2}+r_{ID,3}\beta}$。如果$Z=e(g_{q+1},g')$,则$(u,v,w,y)$是有可用的,$(u,v,w)$对$\mathcal{A}$来说是适当分布的攻击,理由同定理 3.4 证明过程。

阶段 2:$\mathcal{A}$产生密钥查询,然后$\mathcal{B}$按照阶段 1 的描述响应。

猜测过程:最后,敌手输出推断$a',b'\in\{0,1\}$。如果$a=a'$和$b=b'$,$\mathcal{B}$输入出 0(表明$Z=e(g_{q+1},g')$);否则输出 1。

完美模拟:当$Z=e(g_{q+1},g')$,公钥和$\mathcal{B}$发出攻击密文源自一个与真实构建完全相同分布;然而必须表明$\mathcal{B}$发布的私钥具有适当的分布。设I是一个由α,

ID_a 和 $\mathcal{A}$ 所查询身份组成的集合，可以看出 $|I| \leqslant q+1$。为了表明 $\mathcal{B}$ 发布的私钥具有适当的分布，从 $\mathcal{A}$ 的角度足够表明：$\{f(\alpha):\alpha \in I\}$ 的值是一致随机并独立的。但这是由 $f(x)$ 为 q 阶随机多项式这一事实而得出的。

概率分析：如果 $Z=e(g_{q+1},g')$，则模拟是完美的，并且 $\mathcal{A}$ 会有 $1/4+\varepsilon'$ 的概率正确地猜测 (a,b)。或者，Z 是一致随机的，因此 (u,v) 是一致随机的，并且是 $G\times G_T$ 的独立元素。在这种情况下，以 $1-2/p$ 的概率存在不等式：$v \neq e(u,g)^{1/(\alpha-ID_0)}$ 和 $v \neq e(u,g)^{1/(\alpha-ID_1)}$。当存在这些不等式时，$e(u,h_{ID_a})v^{r_{ID_a}}=e(u,(hg^{-r_{ID_a}})^{1/(\alpha-ID_a)})v^{r_{ID_a}}=e(u,h)^{\alpha-ID_a}(v/e(u,g)^{1/(\alpha-ID_a)})^{r_{ID_a}}$ 的值是一致随机的，由于从 $\mathcal{A}$ 角度看 r_{ID_a} 是一致随机的，而且是独立的（除了 w 的值以外），则上等式的值从 $\mathcal{A}$ 角度看也是一致随机并独立的。因此，w 是一致随机而且独立的，而且 (u,v,w) 不能透露出关于值 (a,b) 的任何信息。

假设没有被查询过的身份等于 α（这将只会增加 $\mathcal{B}$ 的成功概率），可以发现当从 R_{ABDHE} 抽取一个样本 $(g',g'_{q+2},g,g_1,\cdots,g_q,Z)$，则 $|Pr[B(g',g'_{q+2},g,g_1,\cdots,g_q,Z)=0]-1/4| \leqslant 2/p$。然而，当从 P_{ABDHE} 抽取样本 $(g',g'_{q+2},g,g_1,\cdots,g_q,Z)$，则有 $|Pr[B(g',g'_{q+2},g,g_1,\cdots,g_q,Z)=0]-1/4| \geqslant \varepsilon'$。因此，对于一致随机的 g,g',α 和 Z，可得 $|Pr[B(g',g'_{q+2},g,g_1,\cdots,g_q,e(g_{q+1},g'))=0]-Pr[B(g',g'_{q+2},g,g_1,\cdots,g_q,Z)=0]| \geqslant \varepsilon'-2/p$。

时间复杂度：在模拟中，$\mathcal{B}$ 的开销主要在计算 $\mathcal{A}$ 对身份 ID 的密钥产生查询 $g^{F_{ID}(\alpha)}$ 上，其中 $F_{ID}(x)$ 是阶为 $q-1$ 的多项式。每一次这样的计算需要在群 G 中进行 $O(q)$ 乘方运算。由于 $\mathcal{A}$ 至多产生 $q-1$ 次这样的查询，则 $t=t'+O(t_{exp}\cdot q^2)$。

参考文献

[1] Abdalla M, Bellare M, Catalano D, et al. Searchable encryption revisited: consistency properties, Relation to anonymous IBE and extensions, Lecture notes in computer science, 2005, Vol. 3621: 205-222.

[2] Boneh D, Boyen X. Efficient selective-ID identity based encryption without random oracles, Lecture notes in computer science, 2004, Vol. 3027: 223-238.

[3] Boneh D, Boyen X. Secure identity based encryption without random oraclesm, Lecture notes in computer science, 2004, Vol. 3152: 443-459.

[4] Boneh D, Boyen X, Goh E -J. Hierarchical identity based encryption with constant size ciphertext, Lecture notes in computer science, 2005, Vol. 3494: 440-456.

[5] Boneh D, Crescenzo G D, Ostrovsky R. Public key encryption with keyword search, Lecture notes in computer science, 2004, Vol. 3027: 506-522.

[6] Boneh D, Franklin M. Identity based encryption from the weil pairing, Lecture notes in

computer science, 2001, Vol. 2139: 213-229.

[7] Boneh D, Gentry C, Waters B. Collusion-resistant broadcast encryption with short ciphertexts and private keys, Lecture notes in computer science, 2005, Vol. 3621: 258-275.

[8] Boneh D, Katz J. Improved efficiency for CCA-secure cryptosystems built using identity based encryption, Lecture notes in computer science, 2005, Vol. 3376: 87-103.

[9] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing, Lecture notes in computer science, 2001, Vol. 2248: 514-532.

[10] Boyen X, Waters B. Anonymous hierarchical identity-based encryption (without random oracles), Lecture notes in computer science, 2006, Vol. 4117: 290-307.

[11] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme, Lecture notes in computer science, 2003, Vol. 2656: 255-271.

[12] Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption, Lecture notes in computer science, 2004, Vol. 3027: 207-222.

[13] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attacks, Lecture notes in computer science, 1998, Vol. 1462: 13-25.

[14] Cramer R, Shoup V. Signature schemes based on the strong RSA assumption, ACM transactions on information and system security, 2000, Vol. 3, No. 3: 161-185.

[15] Dodis Y, Efficient construction of (distributed) verifiable random functions, Lecture notes in computer science, 2002, Vol. 2567: 1-17.

[16] Dodis Y, Yampolskiy A. A verifiable random function with short proofs and keys, Lecture notes in computer science, 2005, Vol. 3386: 416-431.

[17] Gentry C, Silverberg A. Hierarchical ID-based cryptography, Lecture notes in computer science, 2002, Vol. 2501: 548-566.

[18] Horwitz J, Lynn B. Toward Hierarchical identity-based encryption, Lecture notes in computer science, 2002, Vol. 2332: 466-481.

[19] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme, Lecture notes in computer science, 2004, Vol. 3152: 426-442.

[20] Shamir A. Identity-based cryptosystems and signature schemes, Lecture notes in computer science, 1984, Vol. 196: 47-53.

[21] Shoup V. Lower Bounds for discrete logarithms and related problems, Lecture notes in computer science, 1997, Volume 1233: 256-266.

[22] Waters B. Efficient identity-based encryption without random oracles, Lecture notes in computer science, 2005, Vol. 3494: 114-127.

[23] Cocks C. An identity based encryption scheme based on quadratic residues, Lecture notes in computer science, 2001, Vol. 2260: 360-363.

[24] Barreto P, Kim H, Lynn B. Efficient algorithms for pairing-based cryptosystems, Lecture notes in computer science, 2002, Vol. 2442: 354-369.

[25] Bellare M, Desai A, Pointcheval D. Relations among notions of security for public-key

encryption schemes, Lecture notes in computer science, 1998, Vol. 1462: 26-45.

[26] Boneh D. The decision Diffie-Hellman problem, Lecture notes in computer science, 1998, Vol. 1423: 48-63.

[27] Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: security proofs and improvements, Lecture notes in computer science, 2000, Vol. 1807: 259-274.

[28] Coron J. On the exact security of full-domain-hash, Lecture notes in computer science, 2000, Vol. 1880: 229-235.

[29] Desmedt Y, Quisquater J. Public-key systems based on the difficulty of tampering, Lecture notes in computer science, 1986, Vol. 263: 111-117.

[30] Crescenzo G D, Ostrovsky R, Rajagopalan S. Conditional oblivious transfer and timed-release encryption, Lecture notes in computer science, 1999, Vol. 1592: 74-89.

[31] Dolev D, Dwork C, Naor M. Non-malleable cryptography, SIAM Journal on computing, 2000, Vol. 30, No. 2: 391-437.

[32] Feige U, Fiat A, Shamir A. Zero-knowledge proofs of identity, J. Cryptology, 1988, Vol. 1: 77-94.

[33] Fiat A, Shamir A. How to prove yourself: Practical solutions to identi_cation and signature problems, Lecture notes in computer science, 1986, Vol. 263: 186-194.

[34] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes, Lecture notes in computer science, 1999, Vol. 1666: 537-554.

[35] Frey G, Muller M, Ruck H. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, IEEE transactions on information, 1999, Vol. 45: 1717-1718.

[36] Galbraith S. Supersingular curves in cryptography, Lecture notes in computer science, 2001, Vol. 2248: 495-513.

[37] Galbraith S, Harrison K, Soldera D. Implementing the tate-pairing, Lecture notes in computer science, 2002, Vol. 2369: 69-86.

[38] Gemmell P. An introduction to threshold cryptography, RSA laboratories cryptobytes, 1997, Vol. 2, No. 7.

[39] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust and efficient sharing of RSA functions, J. cryptology, 2000, Vol. 13, No. 2: 273-300.

[40] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems, Lecture notes in computer science, 1999, Vol. 1592: 295-310.

[41] Goldreich O, P_tzmann B, Rivest R. Self-delegation with controlled propagation -or-What if you lose your laptop, Lecture notes in computer science, 1998, Vol. 1462: 153-168.

[42] Goldwasser S, Micali S. Probabilistic encryption, J. computer and system sciences, 1984, Vol. 28: 270-299.

[43] Huhnlein D, Jacobson M, Weber D. Towards Practical Non-interactive public key cryptosystems using non-maximal imaginary quadratic orders, Lecture notes in computer

science, 2000, Vol. 2012: 275-287.

[44] Joux A. A one round protocol for tripartite Diffie-Hellman, Lecture notes in computer science, 2000, Vol. 1838: 385-394.

[45] Joux A. The weil and tate pairings as building blocks for public key cryptosystems, Lecture notes in computer science, 2002, Vol. 2369: 11-18.

[46] Joux A, Nguyen K. Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups, J. cryptology, 2003, Vol. 16, No. 4: 239-247.

[47] Maurer U. Towards proving the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, Lecture notes in computer science, 1994, Vol. 839: 271-281.

[48] Maurer U, Yacobi Y. Non-interactive public-key cryptography, Lecture notes in computer science, 1991, Vol. 547: 498-507.

[49] Menezes A, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in afinite field, Information theory, 1993, Vol. 39, No. 5: 1639-1646.

[50] Miyaji A, Nakabayashi M, Takano S. New explicit condition of elliptic curve trace for FRreduction, IEICE Transantions on fundamentals of electronics, communications and computer sciences, 2001, Vol. E84 A, No. 5.

[51] Paillier P, Yung M. Self-escrowed public-key infrastructures in information security and, Lecture notes in computer science, 1999, Vol. 1787: 257-268.

[52] Rackoff C, Simon D. Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack, Lecture notes in computer science, 1991, Vol. 547: 433-444.

[53] Rubin K, Silverberg A. Supersingular abelian varieties in cryptography, Lecture notes in computer science, 2002, Vol. 2442: 336-353.

[54] Tsuji S, Itoh T. An ID-based cryptosystem based on the discrete logarithm problem, IEEE Journal, 1989, Vol. 7, No. 4: 467-473.

[55] Tanaka H. A realization scheme for the identity-based cryptosystem, Lecture notes in computer science, 1987, Vol. 293: 341-349.

[56] Verheul E. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, Lecture notes in computer science, 2001, Vol. 2045: 195-210.

[57] Gennaro R. Halevi S, Rabin T. Secure Hash-and-sign signatures without the random oracle, Lecture notes in computer science, 1999, Vol. 1592: 123-139.

[58] Goldwasser S. Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal on computing, 1988, Vol. 17, No. 2: 281-308.

[59] Gentry C. Practical identity-based encryption without random oracles, Lecture notes in computer science, 2006, Vol. 4004: 445-464.

[60] Zhao K, Hu L, Gong G, et al. Comparison of two sampling-based data collection mechanism for Intrusion Detection System. Proceedings of the 2006 international conference on security and management (SAM'06), June 26-29, 2006, Las Vegas, Nevada, USA.

[61] Gong G, Hu L, Zhao K, et al. SPS-VN: Research on the security Policy system for virtual network. Proceedings of the 2006 international conference on security and management (SAM'06), June 26-29,2006, Las Vegas, Nevada, USA.

[62] 胡德斌,王金玲,于孟涛,林宇,胡亮. 基于身份别名的加入辅助认证方的 IBE 方案,吉林大学学报(工学版), 2008.2,Vol.38, No.2: 419-422.

[63] 陆琳琳,胡亮. MD5 算法及其性能优化. 计算机科学, 2006, Vol. 33, No. 8 增刊: 172-174.

第四章　基于身份的分层加密算法

4.1　基于身份的分层加密算法介绍

2002 年美国密码学家 Gentry 和 Silverberg 在总结了前人研究成果的基础上，第一次提出了一个完整的、建立在随机预言机模型下和双线性 Diffie-Hellman (BDH)假设基础上的基于身份的分层密码算法(HIBC, hierarchical ID-based cryptography)。该方案将私钥生成器(PKG)的功能分为多层，包括一个根 PKG 和多层的域 PKG。根 PKG 只为域 PKG 生成私钥，并对其进行身份认证。域 PKG 在得到私钥之后又可以利用自己的私钥为下层的域 PKG 生成私钥，直至最终用户的上一层，而这一层的 PKG 往往处于用户的本地或局域网中，这就使得对用户的认证和密钥的传输都在本地进行。如果低层 PKG 的密钥泄露，只会影响其域内用户，而不影响高层 PKG 私钥的安全性。

在 Gentry 和 Silverberg 提出的 HIBE 结构中，密文和私钥的长度以及加、解密所需时间都随着层的深度线性增长。2005 年，美国密码学家 Boneh, Boyen 和 Goh 提出了一个密文大小和解密开销与层级深度无关的 HIBE 方案。该方案的密文由三组元素组成，并且解密只需要 2 个双线性对计算。Boneh 等人提出的基础 HIBE 方案中的私钥与之前的 HIBE 结构中的私钥相似，其安全性是基于 BDHE 假设，该假设是 Gentry 对 Diffie-Hellman Inversion 假设的自然扩展。

受 Boneh 等人工作的启发，2006 年 Au 等人提出了一个基于 q-ABDHE 假设的基于身份的分层加密及签名算法，其密文的大小是一个常量，而且公共参数的大小也与表示身份的字符串的长度无关，当这个方案中表示用户身份的 ID 数量增加时，每个身份使用的位数可以相应地减少。同年，Chatterjee 和 Sarkar 对 IBE 进行扩展，提出了只需要很少公共参数的 HIBE，在不使用随机预言机的安全模型下该方案被证明是安全的。但是在他们的方案的结构中，加密和解密需要的时间及私钥和密文的长度随着层次深度的线性增长而增长。在不考虑层次深度的情况下，Chatterjee 和 Sarkar 提出的 HIBE 方案中，密文只有三个群元素而且解密仅需要两次双线性映射计算。Chatterjee 和 Sarkar 留下一个悬而未决的问题：在 HIBE 方案的构建中如何避免或控制 HIBE 许多层次中安全性的指数级的退化。

虽然 Au 等人的方案具有很多优点，但在 2009 年，Hu 等人提出了一个对 Au 等人方案的攻击，证明了 Chatterjee 和 Sarkar 提出的问题仍然没有被很好地解决。在同一篇文章中，Hu 等人又给出了一个密文由 4 个群元素组成，解密仅需要 2 次线性映射计算，且与层次深度无关的 HIBE 方案。作者宣称该 HIBE 方案具有紧密的安全退化，有效的计算性和密文短等优点。与 Au 等人的安全基础相同，Hu 等人的 HIBE 方案同样不是基于随机预言模型，而是基于 q-ABDHE 假设。在效率方面 Hu 等人的方案确实很有竞争力，在安全性方面 Hu 等人证明了他们的 HIBE 方案在 q-ABDHE 假设下与基础的 Gentry IBE 方案相同。但在 2010 年，Park 等人指出 Hu 等人的 HIBE 方案的证明存在问题，其方案是在 Boneh 等人的 HIBE 和 Gentry 的 IBE 方案基础上形成的，其证明策略与 Gentry 的 IBE 方案类似，但 Gentry 的 IBE 背后的证明思想不能直接应用于 Hu 等人的 HIBE 方案中。

本章我们将介绍 Gentry 和 Silverberg 的基于身份的分层密码算法，然后介绍 Boneh，Boyen 和 Goh 的算法，并介绍 Au 等人的算法，Hu 等人对 Au 算法的分析及改进，以及 Park 等人对 Hu 等人算法的分析，使读者对 HIBE 这一正在发展中的理论有一个完整清晰的认识。为了便于理解，我们将介绍一些基本概念。

4.2 基本定义与 HIBE 安全模型

定义 1 身份向量：用户在层次结构中拥有自己的位置，其身份向量的定义为 $(ID_1,\cdots,ID_t)$。在层次结构树中，用户的祖先是根 PKG，用户/低层 PKGs 的身份向量是 $\{(ID_1,\cdots,ID_i):1\leqslant i\leqslant t\}$。

定义 2 Gentry 和 Silverberg 的基于身份的分层加密(HIBE)模型。此 HIBE 方案由五个算法组成：*Root Setup*，*Lower-level Setup*，*Extract*，*Encrypt*，和 *Decrypt*。

Root Setup：根 PKG 选择一个安全参数 K 并返回系统参数 *params* 及根密钥。该系统包括一个参数的消息空间描述 M 和密文空间 C。该系统参数将被公开，而根密钥只有根 PKG 知道。

Lower-Level Setup：低级用户必须获得根 PKG 系统参数。在此 HIBE 方案中，一个低层的用户不允许有任何自己的“低层参数”。但是，这种限制并不阻止低层 PKG 产生它自己的密钥，它可能使用此密钥为它的下层提供私钥。事实上，一个较低层的 PKG 可能会生成一个低层的密钥，或者它可能会为每次 *Extract* 随机生成一次性密钥。

Extract：PKG 利用身份元组 $(ID_1,\cdots,ID_i)$ 根据系统参数及其私钥可以为任何一个子节点计算其私钥。

Encrypt：消息的发送者输入变量 $m\in M$ 和接收者的身份元组 $(ID_1,\cdots,ID_i)$，

从而计算出密文 $c \in C$。

Decrypt:接收者输入变量 $c \in C$ 及其私钥 d,从而解密出明文 $m \in M$。

加密和解密必须满足标准的一致性约束,即当 d 是身份元组 *Extract* 算法生成的私钥时,则:$\forall m \in M$, $Decrypt(params, d, c) = m$,其中 $c = Encrypt(params, ID, m)$。

定义 3 Gentry 和 Silverberg 的分层基于身份签名(HIBS):HIBS 方案由五个算法组成:*Root Setup*, *Lower-level Setup*, *Extract*, *Sign* 和 *Verify*。*Root Setup*, *Lower-level Setup* 和 *Extract* 的基本过程与 HIBE 模型相同。

Sign:签名者输入 *params*,它的私钥 d 以及 $m \in M$,输出一个人签名 $s \in S$。

Verify:验证者输入 *params*,签名者的 *ID* 元组,$m \in M$, $s \in S$ 并输出"有效"或"无效"。

签名和验证必须满足一致性约束,即如果 d 是根据身份元组运行 *Extract* 算法生成的私钥时,则:$\forall m \in M$, $Verify(params, ID, m, s)$ = "有效"。其中 $S = Sign(params, d, m)$。

不再特意区分根 PKG 与域 PKG 后,Gentry 和 Silverberg 的分层基于身份加密(HIBE)模型可简化为 l 层 HIBE 方案。该方案由四个算法组成:*Setup*, *Extract*, *Encrypt*, *Decrypt*。算法规定如下:

Setup:输入安全参数 1^{λ},它生成〈*msk*, *param*〉,其中 *msk* 是随机产生的主密钥,*param* 是相应的公共参数。

Extract:输入身份元组 *ID*(其中 $|ID| < l$),它返回 SK_{ID}(与 *param* 相对应的私钥)。

Encrypt:输入接收方的身份 *ID*(其中 $|ID| < l$)和信息 m,它输出一个与 *param* 对应的密文 σ。

Decrypt:输入接收方 *ID* 的私钥(其中 $|ID| < l$),SK_{ID},和一个签名 σ,它解密为消息 m。

同样,简化后的 l 层的 HIBS 方案由四个算法组成(*Setup*, *Extract*, *Sign*, *Verify*)。

系统建立和私钥提取算法同 HIBE 的相应部分相同。其他的算法是如下所示不同的:

Sign:输入签名者身份的私钥,SK_{ID},以及信息 m,它输出一个与 *param* 相对应的签名 σ。

Verify:输入签名者身份元组 *ID*,一条消息 m 和签名 σ,如果 σ 是与 *ID* 相对应的消息 m 的一个有效的签名则它输出 t,否则输出"$\perp$"。

HIBE 的安全性由两个必要条件组成,也就是,正确性和不可区分性。它们的定义如下:

正确性:我们要求对于任意消息 m,任意私钥 SK_{ID} 和它相对应的身份 ID,都有 $m \rightarrow Decrypt(SK_{ID}, Encrypt(ID, m))$。

不可区分性:如下我们所定义的不可区分性,用来对抗针对 HIBE (IND-ID-CCA)的适应身份和适应选择的密文攻击。

其安全模型由以下的预言机定义:

$KEO(ID)$:将 ID (其中 $|ID| \leqslant l$)作为私钥提取预言机的输入,输出与 msk 对应的私钥 SK_{ID}。

$DO(ID, \sigma)$:将接收方身份 ID (其中 $|ID| \leqslant l$)和密文 σ 作为输入的解密预言机,输出一个信息 m。

游戏定义如下:

(1) (阶段 1)挑战者 S 产生系统参数 $param$ 并将 $param$ 给敌手 $\mathcal{A}$。

(2) (阶段 2)$\mathcal{A}$ 可以任意查询 KEO 和 DO。

(3) (阶段 3)$\mathcal{A}$ 将消息 m_0^*, m_1^* 和身份 ID^* ($|ID^*| \leqslant l$)给 S。S 随机挑选一个 bit 位 b 并返回 $\sigma^* = Encrypt(ID^*, m_b^*)$ 给 $\mathcal{A}$。

(4) (阶段 4)$\mathcal{A}$ 在可以任意查询 $KEO(ID)$ 和 $DO(ID, m)$。

(5) (阶段 5)$\mathcal{A}$ 提供一个猜测值 $\hat{b}$。

如果以下条件为真则 $\mathcal{A}$ 获胜:$\hat{b} = b$,$\mathcal{A}$ 从未在 KEO 预言中查询过 ID^*,且从未在 DO 预言中查询过 (ID^*, σ^*)。

定义 4 选择密文安全。在对 KEO 查询 q_e 次且对 DO 查询 q_d 次的不可分区分游戏中,如果没有敌手能在时间 t 内有至少 ε 的优势,那么此 HIBE 方案是 $(t, \varepsilon, q_e, q_d)$-IND-ID-CCA(选择密文)安全的。

我们说,如果以上的不可区分性游戏中不允许解密预言机查询,那么这个 HIBE 方案只是选择明文安全的(IND-ID-CPA)。

HIBS 的安全性由 2 个必要条件组成,即正确性和存在性不可伪造,它们的定义如下:

正确性:我们要求对于任何消息 m,任何私钥 SK_{ID} 以及它相应的身份 ID 都有 $t \leftarrow Verify(ID, m, Sign(SK_{ID}, m))$。

存在性不可伪造:我们定义的存在性不可伪造是用来对抗针对 HIBS (EU-ID-CMA)的有适应能力的身份和有适应性选择信息攻击,如下游戏所示。我们定义了如下的预言机:

$KEO(ID)$:与 HIBE 中的相同。

$SO(ID, m)$:输入为签名者 ID (其中 $|ID| \leqslant l$)和消息 m 的签名预言机,输出签名 σ 使得 $Verify(ID, m, \sigma) = t$。

游戏的定义如下：

(1)(阶段1)挑战者 S 产生系统参数 $param$ 并将它给敌手 $\mathcal{A}$。

(2)(阶段2)$\mathcal{A}$ 可以任意查询 $KEO(ID)$ 和 $SO(ID,m)$。

(3)(阶段3)$\mathcal{A}$ 将使用签名者身份 ID^*($|ID^*| \leqslant l$)的签名 σ^*,和信息 m^* 传送出去。ID^* 或它的前缀从未成为 KEO 的输入并且 σ^* 也不会成为 $SO(ID^*,M^*)$ 的输出。

如果 $\mathcal{A}$ 完成游戏 $T = Verify(ID^*,m^*,\sigma^*)$,则他赢得该游戏。

定义5 在 EU-ID-CMA 的游戏中对 KEO 查询 q_e 次,且对 SO 查询 q_s 次,如果不存在敌手 $\mathcal{A}$ 在时间 t 内有至少 ε 的优势,则 HIBS 方案是 (t,ε,q_e,q_s)-EU-ID-CMA 安全的。

4.3 Gentry 和 Silverberg 方案

4.3.1 Gentry 和 Silverberg 的 HIBE 方案

设 $level_i$ 是在 i 层上的实体集,K 是 $setup$ 算法的安全参数。

Root Setup:根 PKG 执行群生成算法,生成 q 阶素数群 G_1,G_2 及双线性映射 $e:G_1 \times G_1 \to G_2$。选择任意一个生成元 $P_0 \in G_1$。随机选取 $s_0 \in Z_q^*$,并设置 $Q_0 = s_0P_0$。选择 Hash 函数 $H_1:\{0,1\}^* \to G_1$ 和 $H_2:G_1 \to \{0,1\}^n$,$H_3:\{0,1\}^n \times \{0,1\}^n \to Z_q^*$,$H_4:\{0,1\}^n \to \{0,1\}^n$,$H_1,H_2,H_3,H_4$,作为随机预言。明文空间为 $M = \{0,1\}^*$,密文空间为 $C = G_1^t \times \{0,1\}^n$,其中 t 是接收者的层号,该系统参数 $params$ 为 $G_1,G_2,e,P_0,Q_0,H_1,H_2,H_3,H_4$,根 PKG 密钥是 $s_0 \in Z_q^*$。

Lower-level Setup: $level_t$ 层实体 E_t 选取 $s_t \in Z_q^*$,并将其保存起来作为自己的秘密。

Extract:设 E_t 在 $level_t$ 层,身份元组为 $(ID_1,\cdots,ID_t)$,其中 $(ID_1,\cdots,ID_i)$,$1 < i < t$ 是 E_t 在 $level_i$ 层上的祖先元组,设 S_0 是 G_1 上的一个元素,那么 E_t 的父节点如下：

(1) 计算 $P_t = H_1(ID_1,\cdots,ID_t) \in G_1$。

(2) 设 $S_t = S_{t-1} + s_{t-1}P_t = \sum_{i=1}^{t} s_{i-1}P_i$ 为 E_t 的一个秘密点。

(3) 使用 $Q_i = s_iP, 1 \leqslant i \leqslant t-1$。

Encrypt:使用身份元组 $(ID_1,\cdots,ID_t)$,加密 $m \in M$ 的方法如下：

(1) 计算 $P_i = H_1(ID_1,\cdots,ID_i) \in G_1, 1 \leqslant i \leqslant t$。

(2) 随机选择 $\sigma \in \{0,1\}^n$,计算 $r = H_3(\sigma,m)$。

(3) 生成的密文 $c=[rP_Q, rP_2, \cdots, rP_t, \sigma \oplus H_2(g^r), m \oplus H_4(\sigma)]$，其中 $g=e(Q_0, P_1) \in G_2$。

Decrypt:

(1) 设 $c=[U_0, U_1, \cdots, U_t, V, W] \in C$ 是用身份元组 $(ID_1, \cdots, ID_t)$ 加密的密文。为了解密 c，E_t 计算

$$\sigma = V \oplus H_2\left(\frac{e(U_0, S_t)}{\prod_{i=2}^{t} e(Q_{i-1}, U_i)}\right)$$

(2) 计算 $m=W \oplus H_4(\sigma)$。

(3) 计算 $r=H_3(\sigma, m)$，然后测试 $rP_0, rP_2, \cdots, rP_t, \sigma \oplus H_2(g^r)$ 是否与接收到的密文 c 中的相应字段相同。若不同，则认为密文被篡改。若相同，则接受 m 作为 c 解密出的明文。

Gentry 和 Silverberg 的 HIBE 方案的特点如下：

每个低层 PKG 就像根 PKG 一样拥有密钥 $s_t \in Z_q^*$。低层的 PKG 就像根 PKG 一样使用这个密钥为它的子节点生成密钥，而且低层的 PKGs 对于每次私钥的提取不一定使用相同的 s_t，而是可以每次都使用随机生成的 s_t。H_1 可以换成一个迭代散列函数，P_i 可以通过 $P_i=H_1(P_{i-1}, ID_i)$ 的方式来计算，而不是 $P_i=H_1(ID_1, \cdots, ID_i)$。

4.3.2 Gentry 和 Silverberg 的 HIBS 方案

该方案 HIBS 的安全性是基于 Bilinear Diffie-Hellman 困难问题的。

设 $Level_i$ 是 i 层的实体的集合。其中，$Level_0=\{\text{Root PKG}\}$。$K$ 是 *setup* 算法的安全参数。

Root Setup：根 PKG 执行群生成算法，生成 q 阶素数群 G_1, G_2 及双线性映射 $e: G_1 \times G_1 \rightarrow G_2$。选择任意一个生成元 $P_0 \in G_1$。随机选取 $s_0 \in Z_q^*$，并设置 $Q_0=s_0P_0$。选择 Hash 函数 $H_1: \{0,1\}^* \rightarrow G_1$，$H_3: \{0,1\}^* \rightarrow G_1$，$H_1, H_3$ 作为随机预言，签名的密文空间为 $S=G_1^{t+1}$，其中 t 是接收者的层号，该系统参数 *params* 为 $G_1, G_2, e, P_0, Q_0, H_1, H_3$，根 PKG 密钥是 $s_0 \in Z_q^*$。

Lower-Level Setup 和 *Extract* 算法与前面介绍的 HIBE 算法相同。

Sign：为了用身份元组 $(ID_1, \cdots, ID_t)$ 对消息 m 签名，签名者需要使用自己的秘密点 $S_t=\sum_{i=1}^{t} s_{i-1}P_i$ 及 $Q_i=s_iP_0, 1 \leqslant i \leqslant t$ 执行如下操作：

(1) 计算 $P_m=H_3(ID_1, \cdots, ID_t, m) \in G_1$。

(2) 计算 $Sig(ID_1, \cdots, ID_t, m)=S_t+s_tP_m$。

(3) 发送 $Sig(ID_1, \cdots, ID_t, m)$ 和 $Q_i=s_iP_0(1 \leqslant i \leqslant t)$ 给验证者。

Verify：设 $[Sig, Q_1, \cdots, Q_t] \in S$ 是 $Sig(ID_1, \cdots, ID_t, m)$ 的签名，验证者确认下

面等式是否成立：

$$e(P_0,Sig) = e(Q_0,P_1)e(Q_t,P_M)\prod_{i=2}^{t} e(Q_{i-1},P_i)$$

4.4 Boneh 等人密文长度固定的 HIBE 方案

设 G 为阶为素数 p 的双线性群，并且设 $e:G\times G\to G_1$ 为一个双线性映射。假设层深为 k 的公钥（即一个身份 ID）记为 $ID=(I_1,\cdots,I_k)$。第 j 个分量对应于在 j 层的身份。随后可以使用一个抗碰撞 Hash 函数 $H:\{0,1\}^*\to Z_p^*$ 首先对每个分量 I_j 进行 Hash 运算，从而对 $\{0,1\}^*$ 上的公钥进行扩展构建。

假设要加密的消息是 G_1 中的元素，HIBE 系统工作如下：

Setup：为最大层深为 l 的 HIBE 产生系统参数，选择一个随机生成元 $g\in G$，一个随机的 $\alpha\in Z_p$，并且使得 $g_1=g^\alpha$。接下来，选择随机元素 $g_2,g_3,h_1,\cdots,h_l\in G$。公开参数和主密钥为：

$$pararms = (g,g_1,g_2,g_3,h_1,\cdots,h_l)$$

$$master\text{-}key = g_2^\alpha$$

Extract$(d_{ID_{k-1}},ID)$：为层深 $k\leqslant l$ 的身份 $ID=(I_1,\cdots,I_k)$ 生成私钥 d_{ID}，挑选随机的 $r\in Z_p$ 并输出 $d_{ID}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r,g^r,h_{k+1}^r,\cdots,h_l^r)\in G^{2+l-k}$。

注意 d_{ID} 随着 ID 层深的增长将变得更短。ID 的私钥只能由已知的 $ID_{k-1}=(I_1,\cdots,I_{k-1})$ 的私钥通过请求生成。

事实上，假设 $d_{ID_{k-1}}=(g_2^\alpha\cdot(h_1^{I_1}\cdots h_{k-1}^{I_{k-1}}\cdot g_3)^{r'},g^{r'},h_k^{r'},\cdots,h_l^{r'})=(a_0,a_1,b_k,\cdots,b_l)$ 为 ID_{k-1} 的私钥。生成 d_{ID}，选择一个随机的 $t\in Z_p$ 并且输出 $d_{ID}=(a_0\cdot b_k^{I_k}(h_1^{I_1}\cdots h_{k-1}^{I_{k-1}}\cdot g_3)^t,a_1,g^t,b_{k+1},h_{k+1}^t,\cdots,b_l\cdot h_l^t)$。这个私钥满足 $r=r'+t\in Z_p$，且关于 $ID=(I_1,\cdots,I_k)$ 是随机分布的。

Encrypt$(params,ID,m)$：使用公钥 $ID=(I_1,\cdots,I_k)\in(Z_p^*)^k$ 加密消息 $m\in G_1$，挑选一个随机的 $s\in Z_p$ 并输出 $ct=(e(g_1,g_2)^s\cdot m,g^s,(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^s)\in G_1\times G^2$。

Decrypt(d_{ID},ct)：给定身份 $ID=(I_1,\cdots,I_k)$，使用私钥 $d_{ID}=(a_0,a_1,b_{k+1},\cdots,b_l)$ 解密一个密文 $ct=(A,B,C)$，输出 $A\cdot e(a_1,C)/e(B,a_0)=m$。

事实上，对于一个有效的密文有：

$$\frac{e(a_1,C)}{e(B,a_1)}=\frac{e(g^r,(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^s)}{e(g^s,g_2^\alpha(h_1^{I_1}\cdots h_k^{I_k}\cdot g_3)^r)}=\frac{1}{e(g,g_2)^{s\alpha}}=\frac{1}{e(g_1,g_2)^s}$$

对于任何深度的身份，密文由 3 个元素组成并且解密只需要 2 个对。在之前的 HIBE 系统中，密文大小和解密时间都随着身份的层深呈线性增长。同样，

要注意用于加密的 $e(g_1,g_2)$ 可以重新计算(或在系统参数中替换 g_2),以至加密不需要任何对计算。

4.5 Au 等人的方案

4.5.1 Au 等人的 HIBE 方案

假设 G 和 G_T 是阶为 p 的群,且设 $e:G\times G\rightarrow G_T$ 是双线性映射。G 和 G_T 间的操作用一个乘法符号表示。

Setup:PKG 随机选择生成元 $g\in G$ 且随机选择 $h_1,\cdots,h_l\in_R G,\alpha\in_R Z_p$。它对 $i\in(2,\cdots,l)$ 设置 $g_1=g^{\alpha},u_i=h_i^{\alpha}$。公开参数 *param* 和主密钥 *msk* 由 $param=(g,g_1,h_1,\cdots,h_l,u_2,\cdots,u_l)$ 和 $msk=\alpha$ 得出。

Extract(第一层):为身份 $ID_1\in Z_p$ 生成私钥,PKG 生成随机的 $r_1\in_R Z_p$,计算 $a_1=(h_1g^{-r_1})^{1/(\alpha-ID_1)}$,并且输出私钥$(a_1,r_1)$。

Extract(其他层):为$(ID_1,\cdots,ID_i)\in Z_p^i$ 生成私钥,PKG 生成随机的$i_i\in_R Z_p$,计算 $a_i=a_1\left(\prod_{k=2}^{i}F(k)^{ID_k}\right)^{r_i},b_i=(g_1g^{-ID_1})^{r_i},c_{i,i+1}=F(i+1)^{r_i},\cdots,c_{i,l}=F(l)^{r_i}$,其中 $F(k)=u_kh_k^{-ID_1}$,私钥为$(a_i,b_i,c_{i,i+1},\cdots,c_{i,l},r_1)$。这个私钥也可以由它的私钥为 $a_{i-1},b_{i-1},c_{i-1,i},\cdots,c_{i-1,l}$的父节点$(ID_1,\cdots,ID_{i-1})$来生成。它生成随机的 $t\in_R Z_p$,同时计算

$$a_i=a_{i-1}\cdot c_{i-1,i}^{ID_i}\cdot\left(\prod_{k=2}^{i}F(k)^{ID_k}\right)^{t}$$

$$b_i=b_{i-1}\cdot(g_1g^{-ID_1})^{t}$$

$$c_{i,i+1}=c_{i-1,i+1}\cdot F(i+1)^{t},\cdots,c_{i,l}=c_{i-1,l}\cdot F(l)^{t}$$

这个私钥是满足 $r_i=r_{i-1}+t$,且在值域内随机分布。

Encrypt:使用身份$(ID_1,\cdots,ID_i)\in Z_p^i$ 对 $m\in G_T$ 进行加密,发送方随机选择 $s\in_R Z_p$并构建密文 $c=(C_1,C_2,C_3,C_4)=(g_1^sg^{-sID_1},e(g,g)^s,m\cdot e(g,h_1)^{-s},\left(\prod_{k=2}^{i}F(k)^{ID_k}\right)^{s})$。

Decrypt:用私钥$(a_i,b_i,c_{i,i+1},\cdots,c_{i,l},r_1)$对密文进行解密,以如下方式计算明文:

$$m=C_3\cdot e(C_1,a_i)\cdot C_2^{r_1}/e(b_i,C_4)$$

方案的正确性如下:

$$
\begin{aligned}
& e(C_1,a_i)\cdot C_2^{r_1}/e(b_i,C_4)\\
&= e(g_1^s g^{-sID_1},a_1(\prod_{k=2}^{i}F(k)^{ID_k})^{r_i})\cdot e(g,g)^{sr_1}/e(g_1g^{-ID_1},\prod_{k=2}^{i}F(k)^{ID_k})^{sr_i}\\
&= e(g_1^s g^{-sID_1},a_1)\cdot e(g,g)^{sr_1}\\
&= e(g^{s(\alpha-ID_1)},(h_1g^{-r_1})^{1/(\alpha-ID_1)})\cdot e(g,g)^{sr_1}\\
&= e(g,h_1)^s
\end{aligned}
$$

4.5.2 Au 等人的 HIBS 方案

假设 G 和 G_T 是阶为 p 的群，设 $e:G\times G\to G_T$ 是双线性映射。G 和 G_T 的运算用一个乘法符号表示。

Setup：PKG 随机选择生成元 $g\in G$ 并且随机选择 $h_1,\cdots,h_l\in_R G$ 和 $\alpha\in_R Z_p$。设 $g_1=g_\alpha$，$u_i=h_i^\alpha$，$i\in\{2,\cdots,l\}$。公开参数 *param* 和主密钥 *msk* 如下：

$$param=(g,g_1,h_1,\cdots,h_2,u_2,\cdots,u_l)$$

$$msk=\alpha$$

第一阶段的私钥提取：为身份 $ID_1\in Z_p$ 产生私钥，PKG 产生随机的 $r_1\in_R Z_p$，计算

$$a_1=(h_1g^{-r_1})^{1/(\alpha-ID_1)}$$

并输出私钥 (a_1,r_1)。

其他阶段的私钥提取：为身份 $(ID_1,\cdots,ID_i)\in Z_p^i$ 产生私钥，PKG 生成一个随机的 $r_1\in_R Z_p$，同时计算

$$
\begin{aligned}
a_i &= a_1(\prod_{k=2}^{i}F(k)^{ID_k})^{r_i}\\
b_i &= (g_1g^{-ID_1})^{r_i}\\
c_{i,i+1} &= F(i+1)^{r_i},\cdots,c_{i,e}=F(l)^{r_i}
\end{aligned}
$$

其中，$F(k)=u_kh_k^{-ID_1}$，私钥为 $(a_i,b_i,c_{i,i+1},\cdots,c_{i,l},r_1)$。这个私钥也能被它的上一级含有私钥 $a_{i-1},b_{i-1},c_{i-1,i},\cdots,c_{i-1,l}$ 的 $(ID_1,\cdots,ID_{i-1})$ 生成。它生成随机的 $t\in_R Z_p$，同时计算

$$
\begin{aligned}
a_i &= a_{i-1}\cdot c_{i-1,i}^{ID_i}\cdot(\prod_{k=2}^{i}F(k)^{ID_k})^t\\
b_i &= b_{i-1}\cdot(g_1g^{-ID_1})^t\\
c_{i,i+1} &= c_{i-1.i+1}\cdot F(i+1)^t,\cdots,c_{i,l}=c_{i-1,l}\cdot F(l)^t
\end{aligned}
$$

这个私钥是满足 $r_i=r_{i-1}+t$，且在值域内随机分布。

Sign：使用身份 $(ID_1,\cdots,ID_i)\in Z_p^i$ 的私钥 $(a_i,b_i,e_{i,i+1},\cdots,c_{i,l+1},r_1)$ 对信息

$m \in Z_p^*$ 进行签名，签名者随机选择 $s \in_R Z_p$ 并构建签名

$$\sigma_1 = a_i \cdot c_{i,i+1}^m \cdot \left(F(i+1)^m \prod_{k=2}^{i} F(k)^{ID_k}\right)^s$$

$$\sigma_2 = b_i \cdot (g_1 g^{-ID_1})^s$$

签名为$(\sigma_1, \sigma_2, r_1)$。

Verify：为了验证信息 m 和身份$(ID_1, \cdots, ID_i)$的签名$(\sigma_1, \sigma_2, r_1)$，它比较下面等式是否成立：

$$e(g_1 g^{-ID_1}, \sigma_1) = e(g, h_1) \cdot e(g, g)^{-r_1} \cdot e\left(\sigma_2, F(i+1)^m \prod_{k=2}^{i} F(k)^{ID_k}\right)$$

方案正确性如下：

$$\begin{aligned} e(g_1 g^{-ID_1}, \sigma_1) &= e\left(g^{\alpha - ID_1}, a_i \cdot c_{i,i+1}^m \cdot \left(F(i+1)^m \prod_{k=2}^{i} F(k)^{ID_k}\right)^s\right) \\ &= e(g^{\alpha - ID_1}, a_1) \cdot e\left(g^{\alpha - ID_1}, \left(\prod_{k=2}^{i} F(k)^{ID_k}\right)^{r_1} \cdot F(i+1)^{mr_i} \cdot \left(F(i+1)^m \prod_{k=2}^{i} F(k)^{ID_k}\right)^s\right) \\ &= e\left(g^{\alpha - ID_1}, (h_1 g^{-r_1})^{1/(\alpha - ID_1)}\right) \cdot e\left(\sigma_2, F(i+1)^m \prod_{k=2}^{i} F(k)^{ID_k}\right) \\ &= e(g, h_1) \cdot e(g, g)^{-r_1} \cdot e\left(\sigma_2, F(i+1)^m \prod_{k=2}^{i} F(k)^{ID_k}\right) \end{aligned}$$

4.6 Hu 等人对 Au 等人的 HIBE 和 HIBS 的分析及改进

4.6.1 安全性分析

为了伪造身份 $ID = (ID_1, ID_2, \cdots, ID_i)$ $(2 \leqslant i \leqslant l)$ 和消息的签名，其中$(ID_1, ID_2, \cdots, ID_i)$和 m 是伪造者从身份空间和消息空间独立地随机选择出来的，伪造者从 Z_p 选择 ID_2'，其中 $ID_2' \neq ID_2$，然后向 PKG 查询身份 $ID' = (ID_1, ID_2')$ 的私钥，PKG 向伪造者返回身份 ID' 的私钥$(a_2, b_2, c_{2,3}, \cdots, c_{2,l}, r_1)$，其中 $a_2 = a_1 F(2)^{ID_2' r_2}$，$c_{2,3} = F(3)^{r_2}, \cdots, c_{2,l} = F(l)^{r_2}$，且 $F(K) = u_k h_k^{-ID_1}$。

在获得身份 ID' 的私钥$(a_2, b_2, c_{2,3}, \cdots, c_{2,l}, r_1)$之后，伪造者计算出：

$$a_2' = a_2, b_2' = b_2^{(ID_2'/ID_2)}$$

$$c_{2,3}' = c_{2,3}^{(ID_2'/ID_2)}, \cdots, c_{2,l}' = c_{2,l}^{(ID_2'/ID_2)}$$

很明显，身份(ID_1, ID_2)的有效私钥是$(a_2', b_2', c_{2,3}', \cdots, c_{2,l}', r_1)$，因此伪造者令 $r_2' = ID_2' r_2 / ID_2$：

$$a_2' = a_2 = a_1 F(2)^{ID_2(ID_2' r_2/ID_2)} = a_1 F(2)^{ID_2' r_2'}$$

$$b_2' = b_2^{ID_2'/ID_2} = (g_1 g^{-ID_1})^{ID_2' r_2/ID_2} = (g_1 g^{-ID_1})^{r_2'}$$

$$c_{2,3}' = c_{2,3}^{ID_2'/ID_2} = F(3)^{ID_2' r_2/ID_2} = F(3)^{r_2'}, \cdots,$$

$$c_{2,l}' = c_{2,l}^{ID_2'/ID_2} = F(l)^{ID_2' r_2/ID_2} = F(l)^{r_2'}$$

下一步，伪造者从 Z_p 中随机选取 t_3，并计算：

$$a_3' = a_2' \cdot c_{2,3}'^{ID_3} \cdot \left(\prod_{k=2}^{3} F(k)^{ID_k}\right)^{t_3}$$

$$b_3' = b_2' \cdot (g_1 g^{-ID_1})^{t_3},$$

$$c_{3,4}' = c_{2,4}' \cdot F(4)^{t_3}, \cdots, c_{3,l}' = c_{2,l}' \cdot F(l)^{t_3}$$

很明显，当 $r_3' = r_2' + t_3$ 时，身份 (ID_1, ID_2, ID_3) 的有效私钥为 $(a_3', b_3', c_{3,4}', \cdots, c_{3,l}', r_1)$。

同样，对于所有的 $j(3 \leqslant j \leqslant i)$，敌手可以从 Z_p 中随机选取 t_j，并计算：

$$a_j' = a_{j-1}' \cdot c_{j-1,j}'^{ID_j} \cdot \left(\prod_{k=2}^{j} F(K)^{ID_k}\right)^{t_j}$$

$$b_j' = b_{j-1}' \cdot (g_1 g^{-ID_1})^{t_j}$$

$$c_{j,j+1}' = c_{j-1,j+1}' \cdot F(j+1)^{t_j}, \cdots, c_{j,l}' = c_{j-1,l}' \cdot F(l)^{t_j}$$

很明显，当 $r_j' = r_{j-1}' + t_j$ 时，身份 $(ID_1, ID_2, \cdots, ID_j)$ 的有效私钥为 $(a_j', b_j', c_{j,j+1}', \cdots, c_{j,l}', r_1)$。

最后，当 $r_j' = r_{i-1}' + t_i$ 时，伪造者获得身份 $(ID_1, ID_2, \cdots, ID_i)$ 的有效私钥 a_i'，$b_i', c_{i,i+1}', \cdots, c_{j,i}', r_1$。因此 $ID_2' \neq ID_2$，很明显 $ID' \neq ID$，因此伪造者可以获得不是由 PKG 或 ID 的前缀所生成的 ID 的私钥。使用获得的私钥，伪造者可以构造出身份 ID 对消息 m 的有效签名。

4.6.2　Hu 等人提出的改进 HIBE 方案

Gentry 提出基于 q-ABDHE 假设的 HIBE 方案，设 G 和 G_T 是一个 p 阶循环群，e 是加密双线性映射：$G \times G \rightarrow G_T$，消息空间是 G_T，身份空间是 Z_p，l 是指定为 HIBE 最大层的正整数。

Setup：这个协议是在群 G, G_T 和线性映射 e 的基础上建立的。PKG 从 G 中随机选取生成元 g, g_0，从 G 中随机选取 $g_2, g_3, h_1, h_2, \cdots, h_l, u_1, u_2, \cdots, u_l$，从 Z_p 中随机选取 α, r, u。设 $g_1 = g^{\alpha}, F(k) = u_k h_k^{-u}$，其中 $1 \leqslant k \leqslant l, g_4 = g_1 g^{-u}, g_5 = g_2 g_3^{-u}$，公共参数 $params = \{r, g_0, g, g_4, g_5, F(1), \cdots, F(l)\}$，主密钥是 α, u。

Extract：设 $ID = (ID_1, ID_2, \cdots, ID_i) \in Z_p^i, i \leqslant i \leqslant l$，从 Z_p^* 选取 i，定义 $d_{ID} = (a_0, a_1, b_{i+1}, \cdots, b_l)$，其中：

$$a_0 = (g_0 g^{-r})^{1/(\alpha - u)} \cdot / \left(\prod_{k=1}^{i} F(k)^{ID_k} \cdot g_5\right)^{r_1}$$

$$a_1 = (g_4)^{r_1}$$

$$b_{i+1} = F(i+1)^{r_i}, \cdots, b_l = F(l)^{r_i}$$

其中 d_{ID} 是身份 ID 的私钥。

密钥的授权可以按照以下的操作得到，假设身份 $(ID_1, ID_2, \cdots, ID_{i-1})$ 的私钥是 $(a_0', a_1', b_i, \cdots, b_l)$，为了得到身份 $(ID_1, ID_2, \cdots, ID_i)$ 的私钥 $(a_0, a_1, b_{i+1}, \cdots, b_l)$，首先从 Z_p 中随机选择 t，然后计算出：

$$a_0 = a_0' \cdot b_i^{'ID_i} \cdot \left(\prod_{k=1}^{i} F(k)^{ID_k} \cdot g_5\right)^t$$

$$a_1 = a_1' \cdot (g_4)^t$$

$$b_{i+1} = b_{i+1}' \cdot F(i+1)^t, \cdots, b_l = b_l' \cdot F(l)^t$$

很明显，当 $r_i = r_{i-1}' + t$ 时，身份 $(ID_1, ID_2, \cdots, ID_i)$ 的有效私钥是 $(a_0, a_1, b_{i+1}, \cdots, b_l)$。

Encrypt：设 $ID = (ID_1, ID_2, \cdots, ID_i)$ 是将消息 m 加密的身份，从 Z_p 中随机地选择 s，密文是：

$$ct = (A, B, C, D) = \left(m \times e(g, g_0)^{-s}, e(g, g)^s, (g_4)^s, \left(\prod_{k=1}^{i} F(k)^{ID_k} \cdot g_5\right)^s\right)$$

Decrypt：设 $ct = (A, B, C, D)$ 关于身份 $ID = (ID_1, ID_2, \cdots, ID_i)$ 的密文，$(a_0, a_1, b_{i+1}, \cdots, b_l)$ 是对应的私钥，其中 $1 \leqslant i \leqslant l$。解密步骤如下：

验证 A 和 B 是否在 G_T 中，C 和 D 是否在 G 中，如果这些验证有一个失败，那么返回失败，否则计算出明文 $A \times B^r \times e(C, a_0)/e(a_1, D)$。

4.7 Park 等人对 Hu 等人 HIBE 的安全分析

在分析 Hu 等人的 HIBE 方案之前，首先回顾一下 Gentry 的 IBE 方案的证明思想，以帮助我们理解对 Hu-HIBE 方案的分析。在 Gentry 的方案中，身份 ID 的私钥的产生如下：$d_{ID} = (d_1, d_2) = (r_{ID}, (hg^{-r_{ID}})^{1/(\alpha - ID)})$，并且密文计算如下：

$$ct = (C_1, C_2, C_3) = ((g_1, g^{-ID})^s, e(g, g)^s, m \cdot e(g, h)^{-s})$$

之后就可以用 $C_3 \cdot e(C_1, d_2) \cdot C_2^{d_1}$ 来恢复消息。其安全性是建立在 q-tdABDHE 假设基础上的，其中 q 依赖于敌手提交的私钥查询的次数 q'。令 $q > q'$。在其证明中，(对于挑战者)最关键的思想是为 q 次随机多项式 $f(x) \in Z_p[x]$ 设置 $h = g^{f(\alpha)}$ 来处理 q' 次私钥查询。实际上，当敌手进行 ID 的私钥查询时，对应的密钥计算如下：$d_1 = f(ID)$，$d_2 = g^{(f(\alpha) - f(ID))/(\alpha - ID)}$。

这里 d_1 应该与实际构建的分布相同。为了达到这点，挑战者需要 q 次随机多项式 $f(x)$，q 应该大于 q'。在挑战阶段，敌手输出挑战身份 ID^* 和两条消息

m_0, m_1。挑战者同样能够借助上面的计算产生 ID^* 的私钥 $d_{ID^*} = (d_1^*, d_2^*)$。使用 d_{ID^*} 和其相应的挑战密文 $ct^* = (C_1^*, C_2^*, C_3^*)$ 的构建如下：

$$C_1^* = g'_{q+2}(g')^{-(ID^*)q+2}$$

$$C_2^* = Z \cdot e\left(g', \prod_{i=0}^{q} (g_i)^{F_{ID^*,i}}\right)$$

$$C_3^* = M_b / e(C_1^*, d_2^*)(C_2^*)^{d_1^*}$$

其中，$g'_{q+2} = (g')^{\alpha^{q+2}}$，$g_i = g^{\alpha^i}$，$F_{ID^*,i}$ 是式子 $(x^{q+2} - (ID^*)^{q+2})/(x - ID^*)$ 中项 x^i 的系数。在此过程中，有人可能会认为，既然挑战者能够为挑战身份 ID^* 创建私钥 d_{ID^*}，那么挑战者自己也可以使用 d_{ID^*} 解密挑战密文 ct^*。如果这样行得通，那么挑战者就能在没有和敌手交互的情况下独自解决 q-tdABDHE 问题。这样做实际上行得通吗？也就是，挑战者能在解密算法的帮助下区分目标值 Z 是否变成了 $e(g_{q+1}, g')$ 吗？回答是否定的，要理解其中的原因就需要明白 Gentry 的构建背后的关键思想。

解密行不通的原因是常规解密与区分 Z 是随机或是 $Z = e(g_{q+1}, g')$ 是无关的。常规解密是像 $C_3^* \cdot e(C_1^*, d_2^*)(C_2^*)^{d_1^*}$ 这样执行的。实际上，在解密过程中，插入到 C_2^* 和 C_3^* 之间的 Z 的值被抵消了，这样挑战者就获取不到 Z 的信息了。有两个理由。第一，挑战者将 $(C_2^*)^{d_1^*}$ 和 C_3^* 相乘，在这种情况下 Z 被插入到 C_2^* 中而抵消了。第二，C_1^* 由项 $\{g'_{q+2}, g'\}$ 组成，d_2^* 由项 $\{g_{q-1}, \cdots, g_1, g\}$ 组成。因此由 $e(C_1^*, d_2^*)$ 产生的所有可能的配对的值组成了集合 $\{e(g', g)^{\alpha^i}\}$ 的元素，其中 $k \in \{0, 1, 2q+1\}/\{q, q+1\}$。强调一下，值 $e(g', g)^{\alpha^{q+1}}$ 将不会再出现在 $e(C_1^*, d_2^*)$ 中。这样的结果是，在不考虑值 Z 的情况下使用 d_{ID^*} 解密 ct^*，这就意味着挑战者从常规解密中无法获得 Z 的信息。

不过，在 Gentry 的 IBE 的证明中，可以预测在模拟期间将值 d_1^* 对敌手隐藏是合理的，因为 $f(x)$ 是 q 次随机多项式，在敌手看来，所有关于被查询身份 $\{ID_i\}$ 的 $\{f(ID^*), F(ID_i)\}$ 值都是均匀分布的。这就强制敌手在没有 $d_1^* = f(ID^*)$ 知识的情况下来解密挑战密文 ct^*。在这种情况下，内嵌的值 Z 就不会像以前那样被轻易地得到，因此挑战者利用敌手的能力来攻破 Gentry 的方案。这就是为什么 Gentry 的证明是有效的，相似的问题在 Hu 等人的文献介绍部分也可以发现。对敌手来说，预测用于解密的指数 d_1^* 是困难的。

Hu 等人的安全证明的分析如下：

首先 q-tdABDHE 假设对处理至多 $q-1$ 次私钥查询是没必要的。在他们的模拟中，被查询的身份 $ID = (ID_1, \cdots, ID_i)$ 的私钥可按如下方式产生：

$$a_0 = g^{H(\alpha)}\left(\prod_{k=1}^{i} F(k)^{ID_k} \cdot g_5\right)^{r_i}$$

$$a_1 = (g_4)^{r_i}$$

$$b_{i+1} = F(i+1)^{r_i}, \cdots, b_l = F(l)^{r_i}$$

其中,$H(x) = (f(x) - f(u))/(x-u)$是 $q-1$ 次多项式。这里$f(x)$是 q 次随机多项式,r_i 是由挑战者选择的随机指数。同样,$f(u)$是公开的,而 u 是保密的。为了与 Gentry 的安全性证明对比,u 在 HHF-HIBE 方案中不变。这样挑战者给敌手的随机值(包括$f(u)$)没必要多于 $q-1$ 个。r_i 是由挑战者选择的,并且未知的 α 不包含其中。事实上,从敌手的角度来看要保持值 $f(u)$ 随机,使用 2-tdABDHE 假设(它是静态的)就足够了。那样的话,模拟之间唯一的不同就是使用的是 2 次随机多项式$f(x)$。因此,只要 Hu 等人的安全性证明没有弱点,就可以将 HHF-HIBE 的构建视为一个安全性只依赖于静态假设的新 HIBE 方案。不过,从信息论的观点来看这似乎有些奇怪,因为它的安全性结果应该明显优于 Gentry 的 IBE 方案。而 Hu-HIBE 方案的安全性没有归约到 q-tdABDHE 假设上。于是,可以构建一个安全性能够归约到 Hu 等人 HIBE 方案的安全性修改版本的 HIBE 方案,如下:*Setup* 和 *Extract* 算法与其相同。使用身份 $ID = (ID_1, \cdots, ID_i)$ 对消息 m 进行加密,*Encrypt* 算法输出密文:

$$ct = (A,B,C) = \left(m \cdot e(g,g_0)^{-s} e(g,g)^{rs}, g^s, \left(\prod_{k=1}^{i} F(k)^{ID_k} g_5\right)^s\right)$$

注意:r 是公共参数之一。然后 *Decrypt* 算法输出 $A \cdot e(B,a_0)/e(a_1,C) = m$。事实上,因为 r 是公共的,在 HHF-HIBE 方案中,加密和解密算法都不需要进行与 r 有关的额外的幂运算。从效率的各个方面来考虑,修改后的方案都比原来的 Hu-HIBE 方案更加高效。至于修改后的方案的安全性,结论如下:

断言 1 如果 Hu-HIBE 方案是安全,那么上面修改后的方案也是安全的。

证明:$\mathcal{A}$ 和 $\mathcal{B}$ 分别是要攻击修改后方案和 HHF-HIBE 方案的敌手。$\mathcal{A}$ 提交的私钥查询可以被 $\mathcal{B}$ 提交的私钥查询直接处理掉。在挑战阶段,$\mathcal{A}$ 给 $\mathcal{B}$ 一个身份和两条消息,$\mathcal{B}$ 再将他们转送给它的挑战者。当 $\mathcal{B}$ 接收到它的挑战 $ct = (A,B,C,D)$,$\mathcal{B}$ 重建 $ct' = (\tilde{A} = AB', \tilde{B} = C, \tilde{C} = D)$,并将 ct' 作为挑战密文传送给 $\mathcal{A}$。显然,$\mathcal{B}$ 的优势和 $\mathcal{A}$ 相等。

根据断言 1,可以得到一个新的 IBE 方案,它的效率与 Gentry 的方案相同,尽管如此,在 2-tdABDHE 假设下新 IBE 方案的安全性仍是可证明的。

从信息论的观点来看,如果 HHF-HIBE 是安全的,那么这是一个重要的改进。同时,根据断言 1,推导结果如下:

$$q\text{-tdABDHE} \rightarrow \text{HHF-HIBE} \rightarrow \text{修改后的 HIBE}$$

其中,$A \rightarrow B$ 表示 B 的安全性依赖于 A。因此,如果由 Hu-HIBE 方案完成的归约是正确的,那么修改后的方案的安全性也必能归约到 q-tdABDHE 假设上。将 Hu 等人的证明策略和断言 1 中证明的交互性结合起来可以进行直接归约。不

过接下来的断言表明,直接地归约并不能保持不变。这个矛盾的结果暗示上面两个归约中至少有一个是不正确的。因为断言 1 的归约是使用通用方法完成的,所以可以根据断言 2 得出,Hu 等人的归约是不正确的。

断言 2 使用 Hu 等人的证明策略和断言 1 并不能将修改后方案的安全性归约为 q-tdABDHE 假设。

证明:$\mathcal{A}$ 是攻击修改后方案的敌手。简要地说,这种归约会产生与在 Gentry 的证明中相似的状况,也就是挑战者使用挑战身份 ID^* 产生的私钥来对挑战密文解密时遇到的问题。在挑战阶段,$\mathcal{A}$ 输出挑战身份 $ID^* = (ID_1^*, \cdots, ID_i^*)$ 和两条消息 m_0 和 m_1。首先挑战者使用 Hu 等人的策略构建如下的项:

$$C^* = g'_{q+2}(g')^{-u^{q+2}}$$

$$B^* = Z \cdot e\left(g', \prod_{i=0}^{q}(g_i)^{F_{u,i}}\right)$$

$$A^* = m_b / e(C^*, a_{01}^*)(B^*)^{f(u)}$$

$$D^* = (C^*)^{\beta}$$

其中 $F_{u,i}$ 是项 $(x^{q+2} - u^{q+2})/(x-u)$ 的系数,$a_{01}^* = g^{(f(\alpha)-f(u))/(\alpha-u)}$,$f(u)$ 是公共参数之一,β 是挑战者已知的指数。接着,挑战者计算挑战密文 $ct^* = (\tilde{A}, \tilde{B}, \tilde{C})$,其中:

$$\tilde{A}^* = A^*(B^*)^{f(u)} = m_b / e(C^*, a_{01}^*)$$

$$\tilde{B}^* = C^* = g'_{q+2}(g')^{-u^{q+2}}$$

$$\tilde{C}^* = D^* = (C^*)^{\beta}$$

注意:插入到 B^* 中的 Z 被抵消了。而且,Z 并不在 $e(C^*, a_{01}^*)$ 的结果中出现,因为与 Gentry 的证明中一样,C^* 是由项 $\{g'_{q+2}, g'\}$ 组成的,a_{01}^* 是由项 $\{g_{q-1}, \cdots, g_1, g\}$ 组成的。挑战者将一个与 q-tdABDHE 问题的目标值 Z 无关的挑战密文传送给 $\mathcal{A}$。

在这种情况下,从 $\mathcal{A}$ 来看,Z 是独立的。在 $Z = e(g', g)^{\alpha^{q+1}}$ 和 Z 是随机的情况下,$\mathcal{A}$ 输出的比特位 $b' \in \{0,1\}$ 的分布是一样的。根据 Hu 等人的策略,当且仅当 $b' = b$ 保持为真时挑战者输出 1,其中 b 是由挑战者选取的挑战比特位。在这两种情况下以相同的概率保持 $b' = b$。因此,即使 $\mathcal{A}$ 在攻破修改后方案上有不可忽略的优势,挑战者在解决 q-tdABDHE 问题中 Z 值的区分问题上的优势依然为 0。

参 考 文 献

[1] Barreto P S, Kim H Y, Lynn B, Scott M. Efficient algorithms for pairing-based

cryptosystems, Lecture notes in computer science, 2002, Vol. 2442: 354-368.

[2] Blom R. An optimal class of symmetric key generation systems, Lecture notes in computer science,1984, Vol. 209:335-338.

[3] Blundo C, Santis A D, Herzberg A, et al. Perfectlysecure key distribution for dynamic conferences, Lecture notes in computer science,1993,Vol. 740:471-486.

[4] Boneh D, Franklin M. Identity based encryption from the Weil pairing, Lecture notes in computer science,2001, Vol. 2139:213-229.

[5] Gentry C, Practical identity-based encryption without random oracles, Lecture notes in computer science,2006, Vol. 4404:445-464.

[6] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing, Lecture notes in computer science,2001, Vol. 2248:514-532.

[7] Cocks C. An identity based encryption scheme based on Quadratic Residues, Lecture Notes in Computer Science,2001, Vol. 2260:360-363.

[8] Fujisaki E,Okamoto T. Secure integration of asymmetric and symmetric encryption schemes, Lecture notes in computer science,1999, Vol. 1666:537-554.

[9] Hanaoka G,Nishioka T, Zheng Y, Imai H. An efficient hierarchical identity-based key-sharing method resistant against collusion-attacks, Lecture notes in computer science,1999, Vol. 1716, pp. 348-362.

[10] Hanaoka G, Nishioka T, Zheng Y, Imai H. A hierarchical non-interactive key-sharing scheme with low memory size and high resistance against collusion attacks, The computer journal,2002, Vol. 45, No. 3:293-303.

[11] Horwitz J,Lynn B. Toward hierarchical identity-based encryption, Lecture notes in computer science,2002, Vol. 2332:466-481.

[12] Joux A. A one round protocol for tripartite Diffie-Hellman, Lecture notes in computer science,2000, Vol. 1838:385-394.

[13] Rubin K, Silverberg A. Supersingular abelian varieties in cryptology, Lecture notes in computer science,2002, Vol. 2442:336-353.

[14] Shamir A. Identity-based cryptosystems and signature schemes, Lecture notes in computer science,1984, Vol. 196:47-53.

[15] Boneh D,Boyen X. Efficient selective-ID identity based encryption without random oracles, Lecture notes in computer science,2004, Vol. 3027:223-238.

[16] Boneh D, Boyen X. Short signatures without random oracles, Lecture notes in computer science,2004, Vol. 3027:56-73.

[17] Boneh D, Boyen X, Shacham H. Short group signatures, Lecture notes in computer science,2004, Vol. 3152,pp.41-55.

[18] Boneh D, Franklin M. Identity-based encryption from the weil pairing, Lecture notes in computer science,2001, Vol. 2139:213-29.

[19] Boneh D,Katz J. Improved efficiency for CCA-secure cryptosystems built using identity

based encryption, Lecture notes in computer science,2005, Vol. 3376:87-103.

[20] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme, Lecture notes in computer science,2003, Vol. 2656,255-271.

[21] Boneh D, Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption, Lecture notes in computer science,2004, Vol. 3027,207-222.

[22] Dodis Y, Fazio N. Public key broadcast encryption for stateless receivers, Lecture notes in computer science,2002, Vol. 2696:61-80.

[23] Dodis Y, Yampolskiy A. A verifiable random function with short proofs and keys, Lecture notes in computer science,2005, Vol. 3386:416-431.

[24] Fiat A, Naor M. Broadcast encryption, Lecture Notes in Computer Science, 1993, Vol. 773:480-491.

[25] Gentry C, Silverberg A. Hierarchical ID-based cryptography, Lecture notes in computer science,2002, Vol. 2501:548-566.

[26] Goodrich M, Sun J, Tamassia R. Efficient tree-based revocation in groups of low-state devices, Lecture notes in computer science,2004, Vol. 3152:511-527.

[27] Halevy D, Shamir A. The LSD broadcast encryption scheme, Lecture notes in computer science,2002, Vol. 2442:47-60.

[28] Shoup V. Lower bounds for discrete logarithms and related problems, Lecture notes in computer science,1997, Vol. 1233,256-266.

[29] Waters B. Efficient identity-based encryption without random oracles, Lecture notes in computer science,2005, Vol. 3494:114-127.

[30] Chow S S, Lui L C K, Yiu S, Chow K P. Secure hierarchical identity based signature and its application, Lecture notes in computer science,2004, No. 3269:480-494.

[31] Heng S-H, Kurosawa K. k-Resilient identity-based encryption in the standard model, Lecture notes in computer science,2004, Vol. 2964:67-80.

[32] Abdalla M, Bellare M, Catalano D, et al. Searchable encryption revisited: consistency Properties, relation to anonymous IBE and extensions, Lecture notes in computer science, 2005, Vol,3621:205-222.

[33] Attrapadung N, Chevallier-Mames B, Furukawa J, et al. Efficient identity based encryption with tight security reduction, Lecture notes in computer science,2006, Vol. 4301:19-36.

[34] Boneh D, Boyen X. Secure identity based encryption without random oracles, Lecture notes in computer science,2004, Vol. 3152:443-459.

[35] Boneh D, Boyen X, Goh E-J. Hierarchical identity based encryption with constant size ciphertext, Lecture notes in computer science,2005, Vol. 3495:440-456.

[36] Boneh D, Crescenzo G D, Ostrovsky R, PersiaNo G. Public key encryption with keyword search, Lecture notes in computer science,2004, Vol. 3027:506-522.

[37] Boneh D, Gentry C, Waters B. Collusion-resistant broadcast encryption with short ciphertexts and private keys, Lecture notes in computer science, 2005, Vol. 3621:

258-275.

[38] Boyen X, Waters B. Anonymous hierarchical identity-based encryption (without random oracles), Lecture notes in computer science,2006, Vol. 4117:290-307.

[39] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attacks, Lecture notes in computer science,1998, Vol. 1462:13-25.

[40] Dodis Y. Efficient Construction of (distributed) verifiable random functions, Lecture notes in computer science,2002, Vol. 2567:1-17.

[41] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme, Lecture notes in computer science,2004, Vol. 3152:426-442.

[42] Hu X, Huang S, Fan X. Practical hierarchical identity based encryption scheme without random oracles, IEICE fundamentals of electronics, communications and computer sciences,2009, Vol. E92-A, No.6:1494-1499.

[43] Au M H, Liu J K, Yuen T H, et al. Practical hierarchical identity based encryption and signature schemes without random oracles. http://eprint.iacr.org/2006/368.pdf.

[44] Zhang M, Tang J, Guo D, Hu L, Li Q. Succinct text indexes on large alphabet. Proceedings of the third international conference on theory and applications of models of computation (TAMC2006), May 15-20, 2006, Beijing, China.

[45] Zhao K, Li Q, Kang J, et al. Design and implementation of secure auditing system in linux kernel. Proceedings of 2007 IEEE international workshop on anti-counterfeiting security, identification, April 16-18, 2007, Xiamen China:232-236.

[46] Zhao K, Zhang M, Yang K, Hu L. Data collection for intrusion detection system based on stratified random sampling. Proceedings of 2007 IEEE international conference on networking, sensing and control, 15-17 April, 2007, London, United Kingdom.

[47] Zhao K, Tang K, Guo D, et al. Coordinated attacks detection based on event sequence matching. System and information sciences notes, July 2007, Vol.1, No.3:217-220.

[48] 胡亮,初剑峰,林海群,袁巍,赵阔. IBE 体系的密钥管理机制, 计算机学报,2009.3, Vol.32, No.3:543-551.

第五章　基于无证书的签名算法

5.1　基于无证书签名算法介绍

数字签名是现代密码学中最重要的基本安全元素之一。在传统的公钥签名方案中，签名者的公钥实际上就是随机的字符串，认证中心（CA，certification authority）需要对其进行认证。为了将签名者跟它的公钥进行绑定，传统的公钥签名使用证书的形式，认证中心为证书提供数字签名，而支持证书形式的 PKI 在管理和部署方面是非常困难的。虽然 Shamir 的基于身份签名方案能够消除证书，但是由于可信的第三方 PKG（私钥产生中心）负责管理、产生和分发用户私钥，使得用户的私钥托管成为基于身份签名方案的固有问题。

AI-Riyami 和 Paterson 在 2003 年提出了无证书密码思想，解决了基于身份的密码系统固有的密钥托管问题。与基于身份签名方案中的 PKG 相比，无证书签名方案中的 KGC（密钥生成中心）没有查看用户私钥的权限。KGC 用主密钥和用户的身份产生部分私钥，然后用户使用部分私钥和一些秘密的信息来产生真正的私钥。因为公钥不能根据用户的身份计算出来，所以这个系统已经不是基于身份的密码系统。

但是之后，Huang 等人指出了 Riyami 的方案存在安全缺陷并提出了更安全的方案，Gorantla 和 Saxena，Yap，Heng，goil 等人也提出了一些高效的无证书签名（CLS，certificateless signature）方案，而且这些方案只需要三个或者两个对操作，但是它们都被证明是不安全的，并都被攻破了。随后 Yum 和 Lee 提出了一个无证书签名的通用结构，这个通用结构是基于如下两种属性构建的：传统的数字签名方案和基于身份的签名方案。通过安全分析，Yum 和 Lee 声明如果在 Goldwasser 和 Micali 等人提出的数字签名方案在选择明文攻击时存在不可伪造性，并且在与 Bellare 和 Namprempre 等人定义相似模型的选择明文和身份攻击情况下，基于身份签名方案具有不可伪造性，则通用结构在 KGC 攻击和密钥替代攻击时是安全的。

但是，Hu 和 Wong 发现，Yum 和 Lee 提出的安全需求不足以支持他们的安全声明。即使潜在数字签名方案是安全的，但是对“消息和密钥替代攻击”存在脆弱性时，那么 Yum 和 Lee 提出的无证书签名的通用结构在密钥替代攻击下是

不安全的。并且 Hu 等人举例对此进行了说明。之后 Hu 和 Wong 提出了改进的方案,并证明在这个新的模型是安全的。

2006 年,Zhang 等人提出一种高效安全的、需要进行 4 次对运算的 CLS 方案。之后张富泰等人提出了一个更为高效的 CLS 方案,他们的新方案在验证阶段只需要 3 次对运算。

5.2 基础定义及安全模型

5.2.1 基于无证书签名基本模型

基于无证书签名方案是一个包含 7 个多项式时间算法(*CL_Gen*, *CL_Ext_Partial_Pri_Key*, *CL_Set_Sec_Val*, *CL_Set_Pri_Key*, *CL_Set_Pub_Key*, *CL_Sign*, *CL_Vrfy*)的元组,其中:

CL_Gen:主密钥和参数产生算法,它是一个概率性算法,输入 K 比特的安全参数,返回主密钥 $CLSK^*$ 和参数列表 *params*。

CL_Ext_Partial_Pri_Key:部分私钥提取算法,它是一个确定性算法,输入为用户身份 *id*,参数列表 *params*,主密钥 $CLSK^*$,返回用户 *id* 的部分私钥 CLD_{id}。

CL_Set_Sec_Val:秘密值的生成算法,它是一个概率性算法,输入为参数列表 *params*,用户身份 *id*,返回用户 *id* 的秘密值 CLS_{id}。

CL_Set_Pri_Key:签名密钥产生算法,它是一个确定性算法,输入为参数列表,用户 *id* 的部分私钥 CLD_{id},用户的秘密值 CLS_{id},返回用户 *id* 的私有签名密钥 $CLSK_{id}$。

CL_Set_Pub_Key:认证密钥生成算法,它是一个确定性算法,输入为参数列表,用户的身份 *id*,用户的秘密值 CLS_{id},返回用户 *id* 的公开验证密钥 $CLPK_{id}$。

CL_Sign:签名算法,它是一个概率性算法,输入为消息 m,用户身份 *id*,参数列表,用户的私有签名密钥 $CLSK_{id}$,$CL\_Sign_{params}^{CLSK_{id}}(m)$ 返回签名 α。

CL_Vrfy:认证算法,它是一个确定性算法,输入为参数列表,公开验证密钥 $CLPK_{id}$,消息 m,用户身份 *id* 以及签名 α,$CL\_Vrfy_{params}^{CLPK_{id}}(m, id, \alpha)$ 返回 b,$b=1$ 就意味着签名被接受。

在无证书签名方案中,*CL_Gen* 和 *CL_Ext_Partial_Pri_Key* 由 *KGC* 来执行。部分私钥 CLD_{id} 是由 KGC 通过安全的通道传送给用户 *id*。因为 *CL_Set_Sec_Val*, *CL_Set_Pri_Key* 和 *CL_Set_Pub_Key* 是由用户来执行的,所以在无证书签名方案中并没有固有的用户私钥的托管问题。为了确保方案的正确性,要求所有 $CL\_Sign_{params}^{CLSK_{id}}(\cdot)$ 输出的签名都会被 $CL\_Vrfy_{params}^{CLPK_{id}}(\cdot, id, \cdot)$ 认为有效而接受。

对模型的安全分析,Riyami 对基于身份签名方案的模型进行了扩展,允许敌

手选择身份，并能够提取部分私钥或者完整私钥。此外，由于在无证书签名方案中没有证书，还必须考虑敌手能够用它选择的值替换任何公钥的能力。敌手可以访问的预言有5个。第一个是部分私钥泄露预言 $O^{CL}_{Exp\_Partial}(\cdot)$，它以用户的身份 id 为输入，返回 CLD_{id}。第二个是私钥泄露预言 $O^{CL}_{Exp\_Pri}(\cdot)$，如果用户的身份 id 的公钥还没有被替换，那么 id 就可以作为此预言的输入，返回 $CLSK_{id}$。第三个是公钥广播预言 $O^{CL}_{Bro\_Pub}(\cdot)$，它以用户的身份 id 为输入，返回 $CLPK_{id}$。第四个是公钥替换预言 $O^{CL}_{Rep\_Pub}(\cdot,\cdot)$，输入 $(id, CLPK'_{id})$，将用户 id 的公钥 $CLPK_{id}$ 替换为 $CLPK'_{id}$。第五个是签名预言 $O^{CL}_{Sign}(\cdot,\cdot)$，对于输入 (m,id) 它返回 $CL\_Sign^{CLSK_{id}}_{params}(m)$。

无证书签名方案的安全性是针对两种类型的敌手来刻画的。Type Ⅰ敌手 $\mathcal{A}_{Ⅰ}$ 不能访问主密钥，但是能够替换公钥，提取部分私钥和完整私钥，进行签名问询。当 $\mathcal{A}_{Ⅰ}$ 已经替换了用户 id 的公钥，并请求用户的签名，签名预言将返回一个错误提示。不过如果 $\mathcal{A}_{Ⅰ}$ 向签名预言提交替换后的公钥 $CLPK'_{id}$ 以及相应的秘密信息（CLS'_{id} 或 $CLSK'_{id}$），则签名预言返回正确的应答。Type Ⅱ敌手 $\mathcal{A}_{Ⅱ}$ 在不诚实的 KGC 模型中能够知道主密钥，并且能够自己生成部分私钥，不过，$\mathcal{A}_{Ⅱ}$ 不能替换公钥。

如果 II_{CL} 是一个无证书签名方案。对于任何的敌手，可以执行下面的实验：

$$(CLSK^*, params) \leftarrow CL\_Gen(1^k)$$

$$(M, id, \alpha) \leftarrow A^{O_1(\cdot),O_2(\cdot),O^{CL}_{Exp\_Pri},O^{CL}_{Bro\_Pub},O^{CL}_{Sign}(\cdot,\cdot)}(params, h)$$

其中，对于 $\mathcal{A}_{Ⅰ}$ 来说，$h=\perp$，$O_1(\cdot)=O^{CL}_{Exp\_Partial}(\cdot)$，$O_2(\cdot)=O^{CL}_{Rep\_Pub}(\cdot,\cdot)$；对于 $\mathcal{A}_{Ⅱ}$ 来说，$h=CLSK^*$，$O_1(\cdot)=O_2(\cdot)=\perp$。如果当 $CL\_Vrfy^{CLPK_{id}}_{params}(m,id,\alpha)=1$ 并且 $\mathcal{A}$ 遵守了对它的限制，则说 $\mathcal{A}$ 是成功的。用 $Succ_{\mathcal{A},II_{CL}}(k)$ 表示 $\mathcal{A}$ 成功的概率，如果对于任意 PPT（probabilistic polynomial time）敌手 $\mathcal{A}$ 成功的概率 $Succ_{\mathcal{A},II_{CL}}(k)$ 都是可以忽略的，那么 II_{CL} 是安全的。也就是说，对选择消息攻击该方案具有不可伪造性。

Hu 等人随后简化了 Riyami 等人提出的方案，定义无证书签名方案是一组多项式时间算法，表示为（*MasterKeyGen*, *PartiaKeyGen*, *UserKeyGen*, *CL-Sign*, *CL-Ver*）：

主密钥生成（*MasterKeyGen*）：输入安全参数 1^k（其中 $k\in N$），生成主公/私钥对 (mpk, msk)。

用户部分密钥生成（*PartiaKeyGen*）：输入 msk 和用户身份 $ID\in\{0,1\}^*$，生成了部分私钥。

用户密钥生成（*UserKeyGen*）：输入 mpk 和用户身份 ID，生成用户公/私钥对 (upk, usk)。

无证书签名生成(*CL-Sign*):输入用户私钥 *usk*、用户的部分私钥和消息 $m \in \{0,1\}^*$,生成一个签名 σ。

无证书签名验证(*CL-Ver*):输入 *mpk*、用户身份 *ID*、用户公钥 *upk*、消息 *m* 和签名 σ,返回接受或拒绝。

5.2.2 安全模型

在安全模型中根据定义有五个能被敌手访问的预言:

CreateUser:输入身份 $ID \in \{0,1\}^*$,如果 *ID* 已经存在,不做任何操作。否则,创建 *ID*,生成 $partial\_key_{ID} \leftarrow PartialKeyGen(msk, ID)$,$(upk_{ID}, usk_{ID}) \leftarrow UserKeyGen(mpk, ID)$。

RevealPartialKey:输入身份 *ID*,如果 *ID* 存在,它返回 $partial\_key_{ID}$。否则返回符号 $\perp$。

RevealSecretKey:输入 *ID*,如果 *ID* 存在,返回相应用户私钥 usk_{ID},否则返回符号 $\perp$。

ReplaceKey:输入身份 *ID* 和公/私钥对 (upk^*, usk^*),如果 *ID* 存在,那么用 (upk^*, usk^*) 替换用户 *ID* 原有的公/私钥对;否则不执行任何操作。

Sign:输入身份 *ID* 和消息 $m \in \{0,1\}^*$,如果 *ID* 存在但公/私钥对 (upk_{ID}, usk_{ID}) 没有被取代,那么返回一个有效签名 σ(即 $CL\text{-}Ver(mpk, ID, upk_{ID}, m, \sigma) = 1$),如果 *ID* 不存在,则返回符号 $\perp$,如果用户 *ID* 的公/私钥对被替换为 (upk^*, usk^*),那么返回 $\sigma \leftarrow CL\text{-}Sign(usk^*, partial\_key_{ID}, m)$。

询问预言 *ReplaceKey* 时,usk^* 可以是空字符串,这意味着用户私钥没有被提供。如果 usk^* 是空字符串,并且身份 *ID* 的原始私钥被 usk^* 所替换,则对 *ID* 进行 *RevealSecretKey* 询问时,将返回空字符串。即使 usk^* 不是空字符串,那也不意味 usk^* 是 upk^* 对应的私钥,因此,通过 *Sign* 生成的签名是用替代后的私钥 usk^* 实现的。也就是说签名是非法的。

在对抗模型中定义两种游戏,一个是针对 $\mathcal{A}_{\mathrm{I}}$,另一个是针对 $\mathcal{A}_{\mathrm{II}}$。

Game Ⅰ:设 S_{I} 是游戏的模拟器/挑战者,$k \in \mathbf{N}$ 是安全参数。

(1) S_{I} 执行 $MasterKeyGen(1^k)$ 获得 (mpk, msk)。

(2) S_{I} 对 1^k 和 *mpk* 运行 $\mathcal{A}_{\mathrm{I}}$,$\mathcal{A}_{\mathrm{I}}$ 可以对 *CreateUser*, *RevealPartialKey*, *RevealSecretKey*, *ReplaceKey*, *Sign* 进行询问。

(3) $\mathcal{A}_{\mathrm{I}}$ 输出 (ID^*, m^*, σ^*)。

对于某个 ID^* 如果 $CL\text{-}Ver(mpk, ID^*, upk_{ID^*}, m^*, \sigma^*) = 1$ 并且没有对 (ID^*, m^*) 进行 Sign 询问,那么 $\mathcal{A}_{\mathrm{I}}$ 获胜。但是在 *Game* Ⅰ中 $\mathcal{A}_{\mathrm{I}}$ 不能询问 $RevealPartialKey(ID^*)$ 来获得用户部分私钥 $partial\_key_{ID^*}$。

如果所有 PPT 算法,对于 $\mathcal{A}_{\mathrm{I}}$ 来说赢得比赛的概率是可以忽略的,则无证书签名方案在 *Game* Ⅰ中是安全的。注:在生成伪造签名(ID^*, m^*, σ^*)之前,$\mathcal{A}_{\mathrm{I}}$ 可以 *RevealPartialKey*(ID^*),也可以获得用户私钥 usk_{ID^*}。或询问 *ReplaceKey*(ID^*,·,·),并且代替用户公有密钥 upk_{ID^*}。

Game Ⅱ:在这个游戏中,模拟器 S_{II},与另一个敌手 $\mathcal{A}_{\mathrm{II}}$ 相互作用。整个过程与 *Game* Ⅰ很相似,除了有以下不同外:

(1) 运行 $\mathcal{A}_{\mathrm{II}}$ 时,将 *mpk*,*msk* 给 $\mathcal{A}_{\mathrm{II}}$。

(2) 在 *Game* Ⅱ中 $\mathcal{A}_{\mathrm{II}}$ 不能询问 *RevealSecretKey*(ID^*)来获得用户私钥 usk_{ID^*},也不能询问 *ReplaceKey*(ID^*,·,·)来替代用户公钥 upk_{ID^*}。

如果对于所有 PPT 算法对于 $\mathcal{A}_{\mathrm{II}}$ 来说赢得比赛的概率是可以忽略的,则无证书签名方案在 *Game* Ⅱ中是安全的。

与 Riyami 提出的对抗模型相比,主要不同是 Riyami 提出的模型不允许 $\mathcal{A}_{\mathrm{II}}$ 在 *Game* Ⅱ中询问 *ReplaceKey*。因为 $\mathcal{A}_{\mathrm{II}}$ 总能获得用户部分密钥 $partial\_key_{ID}$,当用户公钥 upk_{ID} 被 $\mathcal{A}_{\mathrm{II}}$ 替换后,$\mathcal{A}_{\mathrm{II}}$ 不能发动攻击。另外的不同是在 Riyami 的模型中 *Game* Ⅰ的额外限制是以下两种之一:

(1) $\mathcal{A}_{\mathrm{I}}$ 不能询问 *RevealPartialKey*(ID^*)来获得用户部分私钥 $partial\_key_{ID^*}$。

(2) $\mathcal{A}_{\mathrm{I}}$ 不能询问 *RevealSecretKey*(ID^*)来获得用户秘密密钥 usk_{ID^*}。也不能询问 *ReplaceKey*(ID^*,·,·)去代替用户公有密钥 upk_{ID^*}。

在简化的模型中,附加约束简化成 $\mathcal{A}_{\mathrm{I}}$ 不能询问 *RevealPartialKey*(ID^*)。只考虑 $\mathcal{A}_{\mathrm{I}}$ 危害到 usk_{ID^*}。或替换 upk_{ID^*}。因为泄露 $partial\_key_{ID^*}$ 的情况已经在 *Game* Ⅱ中考虑到了,所以这种简化并不会降低模型的安全性。

通过进一步分析,Hu 等人指出所有之前的模型都没有专门的预言仅仅破解用户私钥 usk_{ID^*},而不破解用户的部分私钥 $partial\_key_{ID^*}$。而在 Hu 等人的模型中是支持这种情况的。所以 Hu 等人的简化后的模型不但没有降低安全反而比 Riyami 等人的更为安全。

5.3 Riyami 的方案

Riyami 基于可证明安全的 ID-PKC 签名方案提出一个无证书公钥签名方案(CL-PKS)。该方案有 7 个算法:*Setup*, *Partial-Private-Key-Extract*, *Set-Secret-Value*, *Set-Private-Key*, *Set-Public-Key*, *Sign* 和 *Verify*。

Setup:

(1) 输入 k,输出$\langle G_1, G_2, e\rangle$,其中 G_1 和 G_2 是素数 q 阶群,$e: G_1 \times G_1 \rightarrow G_2$ 是

配对函数。

(2) 随机选择 $P \in G_1$。

(3) 随机从 Z_q^* 中选择一个主密钥 s,令 $P_0 = sP$。

(4) 选择 Hash 函数 $H_1: \{0,1\}^* \rightarrow G_1^*$, $H: \{0,1\}^* \times G_2 \rightarrow Z_q^*$。

系统参数 $params = \langle G_1, G_2, e, n, P, P_0, H_1, H \rangle$。主密钥是 $s \in Z_q^*$,消息空间 $M = \{0,1\}^n$,签名空间 $S = G_1 \times Z_q^*$。

Partial-Private-Key-Extract:输入身份 $ID_A \in \{0,1\}^n$,按以下步骤为身份 ID_A 的实体 A 构建部分私钥:

(1) 计算 $Q_A = H_1(ID_A) \in G_1^*$。

(2) 输出部分私钥 $D_A = sQ_A \in G_1^*$。

Set-Secret-Value:将 *params* 和实体身份 ID_A 作为输入,随机选择 $x_A \in Z_q^*$,作为 A 的秘密值。

Set-Private-Key:将 *params*、实体 A 的部分私钥 D_A 和 A 的秘密值 $x_A \in Z_q^*$ 作为输入,计算私钥 $S_A = x_A D_A = x_A s Q_A \in G_1^*$。

Set-Public-Key:将 *params*、实体 A 的秘密值 $x_A \in Z_q^*$ 作为输入,构造 A 的公钥 $P_A = \langle X_A, Y_A \rangle$,其中 $X_A = x_A P, Y_A = x_A P_0 = x_A sP$。

Sign:使用私钥 S_A 对消息 $m \in M$ 进行签名,执行以下步骤:

(1) 选择随机 $a \in Z_q^*$。

(2) 计算 $r = e(aP, P) \in G_2$。

(3) 设 $v = H(m, r) \in Z_q^*$。

(4) 计算 $U = vS_A + aP \in G_1$。

(5) 签名 $\langle U, v \rangle$ 作为输出。

Verify:利用 ID_A 和公钥 $\langle X_A, Y_A \rangle$ 对消息 m 的签名 $\langle U, v \rangle$ 进行验证:

(1) 验证 $e(X_A, P_0) = e(Y_A, P)$ 是否满足;如果不满足,输出 $\perp$ 和终止认证。

(2) 计算 $r = e(U, P) \cdot e(Q_A, -Y_A)^v$。

(3) 验证 $v = H(m, r)$ 是否成立;如果成立,输出有效,否则输出无效。

5.4 Yum 和 Lee 的方案及分析

Yum 和 Lee 提出的无证书签名是一种通用的安全构建方案,是在公钥签名和基于身份签名的基础上形成的。令 $\Pi_{PK} = (PK\_Gen, PK\_Sign, PK\_Vrfy)$ 是满足 Goldwasswer 和 Micali 等人提出的安全标准的公钥签名方案。$\Pi_{IB} = (IB\_Gen, IB\_Ext, IB\_Sign, IB\_Vrfy)$ 是安全的基于身份签名方案。为了避免 Π_{IB} 的密钥托管问题,Yum 和 Lee 使用连续的双签名的思想。具体如下:

$CL\_Gen(1^k)$
$(IBSK^*, params) \leftarrow IB\_Gen(1^k)$;
$CLSK^* \leftarrow IBSK^*$;
Return$(CLSK^*, params)$

$CL\_Ext\_Partial\_Key(id, params, CLSK^*)$
$IBSK_{id} \leftarrow IB\_Ext(id, params, CLSK^*)$;
$CLD_{id} \leftarrow IBSK_{id}$;
Return CLD_{id}

$CL\_Set\_Sec\_Val(params, id)$
$(pk_{id}, sk_{id}) \leftarrow PK\_Gen(1^k)$;
$CLS_{id} \leftarrow (pk_{id}, sk_{id})$;
Return CLS_{id}
$CL\_Set\_Pri\_Key(params, CLD_{id}, CLS_{id})$
Parse CLS_{id} as (pk_{id}, sk_{id});
$CLSK_{id} \leftarrow (CLD_{id}, sk_{id})$;
Return $CLSK_{id}$
$CL\_Set\_Pub\_Key(params, id, CLS_{id})$
Parse CLS_{id} as (pk_{id}, sk_{id});
$CLPK_{id} \leftarrow pk_{id}$;
Return $CLPK_{id}$
$CL\_Sign(m, id, params, CLSK_{id})$
Parse $CLSK_{id}$ as (CLD_{id}, sk_{id});
$\alpha \leftarrow PK\_Sign_{sk_{id}}(m)$;
$\beta \leftarrow IB\_Sign^{CLSK_{id}}_{params}(\alpha, id)$;
Return, $\langle \alpha, \beta \rangle$

$CL\_Vrfy(params, CLPK_{id}, m, id, \langle \alpha, \beta \rangle)$
$b_1 \leftarrow IB\_Vrfy_{params}(\alpha, id, \beta)$;
$b_2 \leftarrow PK\_Vrfy_{CLPK_{id}}(m, \alpha)$;
$b \leftarrow b_1 \& b_2$;
Return b

安全分析:定义上面描述的方案为 Ψ_{CL},它的安全性可以通过 II_{PK}和 II_{IBS}的安全性来证明。

定理 5.1 如果 II_{PK}和 II_{IBS}对选择明文攻击是不可伪造的,则 Ψ_{CL}是一个安全的无证书签名方案。

Yum-Lee 等人的通用结构采用的是 Riyami 提出的 7 步算法的无证书签名方案,但是 Hu-Wong 等人简化了 Yum-Lee 的通用结构,转换成如下形式:

$(mpk, msk) \leftarrow MasterKeyGen(1^k)$
Run$(mpk_{IBS}, msk_{IBS}) \leftarrow Gen_{IBS}(1^k)$;

set $mpk := mpk_{IBS}$ and $msk := \mathrm{msk}_{IBS}$

$partial\_key_{ID} \leftarrow PartialKeyGen(msk, ID)$
Run $sk_{IBS}[ID] \leftarrow UKGen_{IBS}(msk, ID)$;
set $partial\_key_{ID} := \langle sk_{IBS}[ID] \parallel ID \rangle$

$(upk_{ID}, usk_{ID}) \leftarrow UserKeyGen(mpk, ID)$
Run $(pk_{PK}, sk_{PK}) \leftarrow Gen_{IBS}(1^k)$;
set $upk_{ID} := pk_{PK}$ and $usk_{ID} := sk_{PK}$

$\sigma \leftarrow CL\text{-}Sign(usk_{ID}, partial\_key_{ID}, m)$
Run $\sigma_{PK} \leftarrow Sign_{PK}(usk_{ID}, m)$;
set $m' := \langle \sigma_{PK} \parallel ID \rangle$;
run $\sigma_{IBS} \leftarrow Sign_{IBS}(sk_{IBS}[ID], m')$;
set $\langle \sigma_{PK} \parallel \sigma_{IBS} \rangle$

$1/0 \leftarrow CL\text{-}Ver(mpk, ID, upk_{ID}, m, \sigma)$
parse σ into $\langle \sigma_{PK} \parallel \sigma_{IBS} \rangle$;
run $b_1 \leftarrow Ver_{IBS}(mpk, ID, \langle \sigma_{PK} \parallel ID \rangle, \sigma_{IBS})$;
run $b_2 \leftarrow Ver_{PK}(upk_{ID}, m, \sigma_{PK})$;
set output to $b_1 \wedge b_2$

在以上的描述中，$\langle X \rangle$ 代表 X 的二进制编码，符号 $\parallel$ 代表二进制字符串级联，$\wedge$ 代表按位与操作。

密钥代替攻击：Yum-Lee 声称在 Π_{PK} 是 euf-cma 安全的，并且 Π_{IBS} 是 euf_cma_ida 安全的条件下，他们的通用结构能够抵抗 $\mathscr{A}_{\mathrm{I}}$ 和 $\mathscr{A}_{\mathrm{II}}$ 类型攻击。但是，Hu-Wong 等人指出只满足这两个条件不足以确保他们的无证书签名方案安全。通过取代目标用户的公钥，他们说明在 *Game* Ⅰ 中 $\mathscr{A}_{\mathrm{I}}$ 能成功的伪造。因为满足 euf-cma 的传统签名方案 Π_{PK}，即使允许敌手自适应询问关于 (pk_{PK}, sk_{PK}) 的签名预言，但是当敌手只知道公钥 pk_{PK} 而不知道对应的私钥 sk_{PK} 时，也不能伪造消息-签名对 (m, σ)。然而 euf-cma 安全无法确保给予敌手关于 (pk_{PK}, sk_{PK}) 的有效消息-签名对 (m, σ)，它不能得到 (σ, m', pk') 使得 $m' \neq m, pk' \neq pk_{PK}$ 但 $Ver_{PK} = (pk', m', \sigma) = 1$。具体如下：

(1) $\mathscr{A}_{\mathrm{I}}$ 任意选择身份 $ID \in \{0,1\}^*$，并询问 $CreateUser(ID)$ 来“创建”相应的用户，假设返回的用户公钥是 pk_{PK}。

(2) 然后 $\mathscr{A}_{\mathrm{I}}$ 任意选择消息 $m \in \{0,1\}^*$，并询问 $Sign(ID, m)$。假设预言返回的签名是 $\sigma = \langle \sigma_{PK} \parallel \sigma_{IBS} \rangle$。

(3) $\mathscr{A}_{\mathrm{I}}$ 生成 (σ, m', pk') 使得 $m' \neq m, pk' \neq pk_{PK}$ 但 $Ver_{PK} = (pk', m', \sigma_{PK}) = 1$。

(4) $\mathcal{A}_I$ 通过 $ReplaceKey(ID, pk', \lambda)$ 来改变 ID 的公钥，其中 λ 是空字符串，表示替代用户公钥对应的私钥。

(5) 最后 $\mathcal{A}_I$ 输出 (ID, m', σ)。

通过以上的分析，他们改进了 Yum-Lee 的签名生成算法，并得出以下结论：

$\sigma \leftarrow CL\text{-}sign(usk_{ID}, partial\_key_{ID}, m)$
set $m' := \langle m \parallel mpk \parallel ID \parallel upk_{ID} \rangle$;
run $\sigma_{PK} \leftarrow Sign_{PK}(usk_{ID}, m')$;
set $m^* := \langle m \parallel mpk \parallel ID \parallel upk_{ID} \parallel \sigma_{PK} \rangle$
run $\sigma_{IBS} \leftarrow Sign_{IBS}(sk_{IBS}[ID], m^*)$;
set $\sigma := \langle \sigma_{PK} \parallel \sigma_{IBS} \rangle$

定理 5.2 如果 IBS 方案 $\Pi_{IBS} = (Gen_{IBS}, UKGen_{IBS}, Sign_{IBS}, Ver_{IBS})$ 满足 euf-cma-ida 安全，改进后的通用结构能够抵抗 *Game* Ⅰ类型攻击。

定理 5.3 如果签名方案 $\Pi_{PK} = (Gen_{PK}, UKGen_{PK}, Sign_{PK}, Ver_{PK})$ 满足 euf-cm 安全，改进后的通用结构能够抵抗 *Game* Ⅱ类型攻击。

5.5 Zhang 等人的方案及安全性分析

5.5.1 Zhang 等人的高效 CLS 方案

Setup：令 G_1 是一个由 P 生成的素数 q 阶循环加法群，G_2 是一个同阶的循环乘法群。$e: G_1 \times G_1 \rightarrow G_2$ 是一个双线性对。KGC 选择一个随机数 $t \in Z_q^*$ 作为主密钥(master key)并设置 $P_{pub} = tP$，选取 Hash 函数 $H: \{0,1\}^* \rightarrow G_1, H_1: \{0,1\}^* \rightarrow Z_q, H_2: \{0,1\}^* \rightarrow G_1^*$。系统参数 $param = (G_1, G_2, e, P, P_{pub}, H, H_1, H_2)$。

Partial-Private-Key-Extract：接受用户身份 ID_i 作为输入，构建用户的部分私钥 $D_i = tQ_i$，其中 $Q_i = H(ID_i)$。

Set-Secret-Value：以用户的身份 ID_i 为输入，选择 $x_i \in_R Z_q^*$ 并输出用户的私密值 x_i。

Set-Private-Key：以用户的部分密钥 D_i 和私密值 x_i 为输入，为用户输出私钥 $S_i = (x_i, D_i)$。

Set-Public-Key：接受用户的私密值 x_i，并产生公钥 $P_i = x_i P$。

Sign：使用私钥 S_i 对消息 m 签名，签名者执行下面的步骤：

(1) 选择 $r \in_R Z_q^*$，计算 $R = rP$。

(2) 计算 $h = H_1(m, R, P_i), U = H_2(m, P_i), S = r(P_{pub} + U) + h(D_i + x_i U)$。

(3) 输出 (R, S) 作为对 m 的签名。

Verify:签名者身份 ID_i 和它的公钥 P_i,要验证对消息 m 的签名 (R,S),验证者执行下面的步骤:

(1) 计算 $Q_i = H(ID_i)$, $U = H_2(m, P_i)$, $h = H_1(m, R, P_i)$。

(2) 检查等式 $e(S,P) = e(R + hQ_i, P_{pub})e(R + hP_i, U)$ 是否成立。如果是,那么输出 *true*;否则,输出 $\perp$。

5.5.2 安全性证明

定理 5.4 在随机预言模型下,如果 Type Ⅰ 敌手 $\mathcal{A}_{\mathrm{I}}$ 能够在时间段 τ 内以 $\varepsilon \geqslant 10(q_k+1)((q_k+1)/q_k)^{q_k}(q_S+1)(q_S+q_H)^{q_S}/2^l$ 的优势攻破这一 CLS 方案,而且至多进行 q_k 次 *Partial-Private-Key* 问询,q_H 次 H_1 问询,q_S 次 *Sign* 问询,那么就存在一个算法 $\mathcal{C}$,它能够在预期的时间 $\tau' = 120686q_H(q_k+1)((q_k+1)/q_k)^{q_k}\tau/\varepsilon$ 内在 G_1 中解决 CDH 问题。

证明:令 $\mathcal{C}$ 是 CDH 攻击者,它收到一个随机实例 (P, aP, bP),并在 G_1 中计算 abP 的值。$\mathcal{A}_{\mathrm{I}}$ 是 Type Ⅰ 敌手,为了说明 $\mathcal{C}$ 是怎么使用 $\mathcal{A}_{\mathrm{I}}$ 来解决 CDH 问题的,首先,$\mathcal{C}$ 设置 $P_{pub} = aP$ 和 $param = (G_1, G_2, e, P, P_{pub}, H, H_1, H_2)$,然后它将 *param* 发送给 $\mathcal{A}_I$。将 Hash 函数 H, H_1 和 H_2 当成随机预言。

H 查询:$\mathcal{C}$ 维护元组 (ID_j, d_j, Q_j, c_j) 的列表 *HList*。一旦接收到对身份 ID_i 的问询,如果在 *HList* 中存在元组 (ID_i, d_i, Q_i, c_i),那么 $\mathcal{C}$ 返回 Q_i 作为应答;否则,$\mathcal{C}$ 首先选择一个 $d_i \in_R Z_q^*$,然后选取 $c_i \in \{0,1\}$ 并且等于 0 的概率为 δ,等于 1 的概率为 $1-\delta$。如果 $c_i = 0$,那么 $\mathcal{C}$ 设置 $Q_i = d_iP$;否则 $c_i = 1$,设置 $Q_i = d_ibP$。在这两种情况下,$\mathcal{C}$ 都会将 (ID_i, d_i, Q_i, c_i) 添加到 *HList* 中,并将 Q_i 返回给 $\mathcal{A}_{\mathrm{I}}$。

H_1 查询:$\mathcal{C}$ 保持元组 (m_j, R_j, P_j, e_j) 的列表 H_1List。只要 $\mathcal{A}_{\mathrm{I}}$ 向 H_1 提交一个 (m_i, R_i, P_i),$\mathcal{C}$ 首先检查在 H_1List 中是否存在元组 (m_i, R_i, P_i, e_i)。如果有,那么 $\mathcal{C}$ 就返回 e_i;否则 $\mathcal{C}$ 就挑选 $e_i \in_R Z_q^*$,然后返回 e_i,并将 (m_i, R_i, P_i, e_i) 添加到 H_1List 中。

H_2 查询:$\mathcal{C}$ 保持元组 (m_j, P_j, f_j, U_j) 的列表 H_2List。只要 $\mathcal{A}_{\mathrm{I}}$ 向 H_2 提交一个 (m_i, P_i),$\mathcal{C}$ 首先检查在 H_2List 中是否存在元组 (m_i, P_i, f_i, U_i)。如果有,那么 $\mathcal{C}$ 就返回 U_i;否则 $\mathcal{C}$ 就挑选 $f_i \in_R Z_q^*$,并设置 $U_i = f_iP$,然后返回 U_i,并将 (m_i, P_i, f_i, U_i) 添加到 H_2List 中。

部分私钥查询:$\mathcal{C}$ 保持元组 (ID_j, x_j, D_j, P_j) 的列表 *KList*,当 $\mathcal{A}_I$ 提交关于 ID_i 的部分私钥问询时,$\mathcal{C}$ 操作如下:

(1) 如果在 *KList* 中存在元组 (ID_i, x_i, D_i, P_i) 并且 $D_i \neq \perp$,那么将 D_i 返回作为应答;否则如果存在元组 (ID_i, x_i, D_i, P_i) 并且 $D_i = \perp$,首先产生关于 ID_i 的 H 问询,然后在 *HList* 中寻找 (ID_i, d_i, Q_i, c_i)。如果 $c_i = 0$,那么设置 $D_i = d_iP_{pub}$,返

回 D_i;否则 $c_i=1$,终止。

(2) 否则,首先产生 $H(ID_i)$,然后在 *HList* 中查找(ID_i,d_i,Q_i,c_i)。如果 $c_i=0$,那么设置 $D_i=d_iP_{pub}$,设置 $x_i=\perp$,$P_i=\perp$,返回 D_i 并将(ID_i,x_i,D_i,P_i)添加到 *KList* 中;否则 $c_i=1$,终止。

公钥查询:一旦接到关于 ID_i 的公钥问询,$\mathscr{C}$检查 *KList*,如果存在元组(ID_i,x_i,D_i,P_i)并且 $P_i\neq\perp$,$\mathscr{C}$返回 P_i,而 $P_i=\perp$时,$\mathscr{C}$选择 $u_i\in_R Z_q^*$,设置$x_i=u_i,P_i=x_iP$ 并返回 P_i。否则,在 *KList* 中没有元组(ID_i,x_i,D_i,P_i),$\mathscr{C}$挑选$u_i\in_R Z_q^*$,设置 $x_i=u_i,P_i=x_iP,D_i=\perp$,返回 P_i,并将(ID_i,x_i,D_i,P_i)添加到 *KList* 中。

私钥查询:一旦接到关于身份 ID_i 的问询,$\mathscr{C}$首先产生关于 ID_i 的部分私钥和公钥问询,如果 $\mathscr{C}$没有终止,就返回(x_i,D_i)。

公钥替换查询:一旦接到公钥替换问询(ID_i,P_i'),$\mathscr{C}$首先产生关于 ID_i 的部公钥查询,然后在 *KList* 中查找元组(ID_i,x_i,D_i,P_i)并设置 $x_i=\perp$,$P_i=P_i'$。

签名查询:一旦接到关于(m_i,ID_i,P_i')的签名问询,$\mathscr{C}$产生签名如下:

挑选 $\tau_i,h_i\in_R Z_q^*$ 并计算 $R_i=\tau_iP-h_iQ_i$,其中 $Q_i=H(ID_i)$,设置 $H_1(m_i,ID_i,P_i)=h_i$。

在 H_2*List* 中查寻元组(m_i,P_i,f_i,U_i)(如果元组不存在,$\mathscr{C}$首先产生 $H_2(m_i,P_i)$)并计算 $S_i=r_iP_{pub}+f_i(R_i+h_iP_i)$。

返回(R_i,S_i)作为应答。

解决 CDH 问题:令$\{m^*,(R,S),ID^*,P^*\}$是 $\mathscr{A}_{\mathrm{I}}$ 在攻击的最后产生的伪造。根据分叉引理,$\mathscr{C}$可以使用相同的随机录像但使用不同的 Hash 函数 H_1' 重放 $\mathscr{A}_{\mathrm{I}}$,以此取得另外一个伪造$\{m^*,(R,S'),ID^*,P^*\}$。从这两个伪造中,$\mathscr{C}$得到$e(S,P)=e(R+hQ^*,P_{pub})e(R+hP^*,U)$和 $e(S',P)=e(R+h'Q^*,P_{pub})e(R+h'P^*,U)$。根据这两个等式,可得 $e(S-S',P)=e(R+hQ^*-(R+h'Q^*),P_{pub})e(R+hP^*-(R+h'P^*),U)$。其中,$U=H_2(m^*,P^*)$,$Q^*=H(ID^*)$和 $h=H_1(m^*,R,P^*)$,$h'=H_1'(m^*,R,P^*)$,其中 $h\neq h'$。

$\mathscr{C}$从 H_2*List* 恢复(m^*,P^*,f,U),从 *HList* 恢复(ID^*,d,Q^*,c)。因为 $Q^*=H(ID^*)$被设置为 dbP,$U=H_2(m^*,P^*)=fP$ 和 $P_{pub}=aP$,根据上面的等式,$\mathscr{C}$有 $S-S'=(h-h')dabP+(h-h')fP^*$。因此,$\mathscr{C}$能得出 $abP=d^{-1}((h-h')^{-1}(S-S')-fP^*)$,这就是 CDH 问题的解。

现在可以确定 δ 的值。$\mathscr{C}$在所有 q_k 次的部分私钥问询都不会失败的概率是 δ^{q_k}。$\mathscr{A}_{\mathrm{I}}$ 伪造的签名但是 $\mathscr{C}$并不知道选定身份的对应的部分私钥的概率是 $1-\delta$。所以组合起来的概率是 $\delta^{q_k}(1-\delta)$。当 $\delta=q_k/(q_k+1)$时概率的取值达到最大,为$(q_k/(q_k+1))^{q_k}/(q_k+1)$。

在从分叉引理得出的边界和上面的概率的基础上，如果 $\mathcal{A}_{\mathrm{I}}$ 在时间 $\leqslant\tau$ 内成功的概率达到 $\varepsilon\geqslant 10(q_k+1)((q_k+1)/q_k)^{q_k}(q_S+1)(q_S+q_H)/2^l$，那么 $\mathcal{C}$ 就能在预期的 $\tau'=120686q_H(q_k+1)((q_k+1)/q_k)^{q_k}\tau/\varepsilon$ 时间内解决 CDH 问题。

定理 5.5 在随机预言模型下，如果 Type Ⅱ 敌手 $\mathcal{A}_{\mathrm{II}}$ 能够在时间段 τ 内以 $\varepsilon\geqslant 10(q_k+1)((q_k+1)/q_k)^{q_k}(q_S+1)(q_S+q_H)^{q_S}/2^l$ 的优势攻破此 CLS 方案，而且至多进行 q_k 次 *Private-Key* 问询，q_H 次 H_1 问询，q_S 次 *Sign* 问询，那么就存在一个算法 $\mathcal{C}$，它能够在预期的时间 $\tau'=120686q_H(q_k+1)((q_k+1)/q_k)^{q_k}\tau/\varepsilon$ 内在 G_1 中解决 CDH 问题。

证明：定理 5.5 的证明和定理 5.4 的证明类似。因此，这里只简要地描述一下 $\mathcal{C}$ 是怎么能用 $\mathcal{A}_{\mathrm{II}}$ 来计算 abP 的（注意 $\mathcal{C}$ 能访问主密钥并把它传给 $\mathcal{A}_{\mathrm{II}}$）。令 $\{m^*,(R,S),ID^*,P^*\}$ 是 $\mathcal{A}_{\mathrm{II}}$ 在攻击的最后输出的伪造（在模拟期间，$\mathcal{C}$ 设置 $P^*=x^*bP, U^*=H_2(m^*,P^*)=faP$）。使用分叉引理技术，$\mathcal{C}$ 可以使用相同的随机录像但使用不同的 Hash 函数 H_1' 重放 $\mathcal{A}_{\mathrm{II}}$，以此取得另外一个伪造 $\{m^*,(R,S'),ID^*,P^*\}$。从这两个伪造中，$\mathcal{C}$ 能够得出 $abP=(fx^*)^{-1}((h-h')^{-1}(S-S')tQ^*)$。

参考文献

[1] Zhang L, Zhang F, Huang X. A secure and efficient certificateless signature scheme using bilinear pairing, Chinese journal of electronic, 2009, Vol. 18, No. 1: 145-148.

[2] Shamir A. Identity based cryptosystems and signature schemes, Lecture notes in computer science, 1985, Vol. 196: 47-53.

[3] Al-Riyami S, Paterson K. Certificateless public key cryptography, Lecture notes in computer science, 2003, Vol. 2894: 452-473.

[4] Gorantla M, Saxena A. An efficient certificateless signature scheme, Lecture notes in computer science, 2005, Vol. 3802: 110-116.

[5] Huang X, Susilo W, Mu Y, Zhang F. On the security of a certificateless signature scheme, Lecture notes in computer science, 2005, Vol. 3810: 13-25.

[6] Li X, Chen K, Sun L. Certificateless signature and proxy signature schemes from bilinear pairings, Lithuanian mathematical journal, 2005, Vol. 45: 76-83.

[7] Yap W, Heng S, Goil B. An efficient certificateless signature scheme, Lecture notes in computer science, 2006, Vol. 4097: 322-331.

[8] Zhang Z, Wong D, Xu J, Feng D. Certificateless public key signature: security model and efficient construction, Lecture notes in computer science, 2006, Vol. 3989: 293-308.

[9] Yum D, Lee P. Generic construction of certificateless signature, Lecture notes in computer science, 2004, Vol. 3108: 200-211.

[10] Pointchevai D, Stern J. Security proofs for signature schemes, Lecture notes in computer science,1996, Vol. 1070:387-398,

[11] Huang X, Susilo W, Mu Y, Zhang F. On the security of certificateless signature schemes from asiacrypt 2003, Lecture notes in computer science,2005, Vol. 3810:13-25.

[12] Al-Riyami S S, Paterson K G. CBE from CLPKE: A generic construction and efficient schemes, Lecture notes in computer science,2005, Vol. 3386:398-415.

[13] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing, Lecture notes in computer science,2005, Vol. 3650:134-148.

[14] Cheng Z, Comley R. Efficient certificateless public key encryption, Lecture notes in computer science,2007, Vol. 4575:83-107.

[15] Girault M. Self-Certified Public Keys, Lecture notes in computer science,1992, Vol. 547: 490-497.

[16] Goldwasser S, Micali S, Rivest R. A secure digital signature scheme, SIAM Journal on computing,1988, Vol. 17:281-308.

[17] Okamoto E. Key distribution systems based on identification information, Lecture notes in computer science,1987, Vol. 293:194-202.

[18] Saeednia S. Identity-based and self-certified key-exchange protocols, Lecture notes in computer science,1997, Vol. 1270:303-313.

[19] Shamir A. Identity-based cryptosystems and signature schemes, Lecture notes in computer science,1985, Vol. 196:47-53.

[20] Boneh D, Franklin M. Identity based encryption from the weil pairing, SIAM Journal of computing,2003, Vol. 32, No. 3:586-615.

[21] Cha J C, Cheon J H. An Identity-based signature from gap Diffie-Hellman groups, Lecture notes in computer science,2003, Vol. 2567:18-30.

[22] Guillou L C, Quisquater J J. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, Lecture notes in computer science,1988, Vol. 330:123-128.

[23] Hu B C, Wong D S, Zhang Z, Deng X. Key replacement attack against a generic construction of certificateless signature, Lecture notes in computer science, 2006, Vol. 4058:235-246.

[24] Bellare M, Namprempre C, Neven G. Security proofs for identity-based identification and signature schemes, Lecture notes in computer science,2004, Vol. 3027:268-286.

[25] Blake-Wilson S, Menezes A. Unknown key-share attacks on the station-tostation (STS) protocol, Lecture notes in computer science,1999, Vol. 1560:154-170.

[26] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. inform. theory,1985, Vol. 31, No. 4:469-472.

[27] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attack, SIAM Journal computing,1988, Vol. 17, No. 2:281-308.

[28] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes, Lecture notes in computer science,1999, Vol. 1666:537-554.

[29] Galindo D, Morillo P, Rafols C. Breaking Yum and Lee generic constructions of certificate-less and certificate-based encryption schemes, Lecture notes in computer science,2006, Vol. 4043:81-91.

[30] Libert, Quisquater J. On constructing certificateless cryptosystems from identity based encryption, Lecture notes in computer science,2006, Vol. 3958:474-490.

[31] Yum H, Lee P J. Identity-based cryptography in public key management, Lecture notes in computer science,2004, Vol. 3093:71-84.

[32] Zhang Z, Wong D, Xu J, Feng D. Certificateless public-key signature: security model and efficient construction, Lecture notes in computer science, 2006, Vol. 3989:293-308.

[33] Bellare M, Desai A, Pointcheval D, Rogaway P. Relations among notions of security for public-key encryption schemes, Lecture notes in computer science, 1998, Vol. 1462:26-45.

[34] Huhnlein, Jacobson M, Weber D. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders, Lecture notes in computer science,2000, Vol. 2012:275-287.

[35] Tsuji S, Itoh T. An ID-based cryptosystem based on the discrete logarithm problem, IEEE Journal on selected areas in communication, 1989, Vol. 7, No. 4:467-473.

[36] Boneh, Boyen X. Short signatures without random oracles, Lecture notes in computer science,2004, Vol. 3027:416-432.

[37] Canetti R, Goldreich O, Halevi S. The random oracle methodology, Journal of the ACM, 2004, Vol. 51, No. 4:557-594.

[38] Waters. Efficient identity-based encryption without random oracles, Lecture notes in computer science,2005, Vol. 3494:114-127.

[39] Joux A. A one round protocol for tripartite Diffie-Hellman, Lecture notes in computer science,2000, Vol. 1838:385-394.

[40] Okamoto M T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field, IEEE transaction on information theory,1993, Vol. 39:1639-1646.

[41] Hu L, Nurbol, Liu Z, He J, Zhao K. A time-stamp frequent pattern-based clustering method for anomaly detection, IETE Technical review,2010, Vol. 27, No. 3:220-227.

[42] Zhao K, Nurbol, Shi G, Hu L. HSTCP: A high-speed traffic collection platform for intrusion detection/prevention based on sampling on FPGAs, IETE Technical review,2010, Vol. 27, No. 3:235-243.

[43] Hu D, Che X, Duan K T Y, Hu L. Dynamic clonal selection algorithm based on artificial immune mechanism. Proceedings of the 1st international conference of ICT innovation and application (ICIIA 2007), Zhuhai, China, Nov 15-17:49-53.

[44] Zhao K, Tang K, Hu D, Hu L. Packet selection model for intrusion detection system based-on sampling. Proceedings of the 1st International conference of ICT Innovation and application (ICIIA 2007), Zhuhai, China, Nov 15-17:104-109.

第六章　基于无证书的加密算法

6.1　基础介绍

2003 年 AI-Riyami 和 Paterson 等人提出了一个新的公钥体制模型，称之为无证书公钥密码体制（CL-PKC，certificateless public key cryptosystem）。无证书公钥密码体制的思想就是既不需要证书也不存在 ID-PKC 的密钥托管问题，它是介于传统 PKI 和 ID-PKI 的公钥体制之间的模型，也就继承了这两种公钥密码体制的一些特性。Riyami 等人在 CL-PKC 中采用了自认证密钥技术和 Gentry 提出的基于证书加密的一些思想。

在新的模型中，可以通过加密、签名和密钥交换这些方面来证实 CL-PKC 是有效和安全的，并且也可以证明分层的无证书方案是可行的。无证书方案也是基于双线性映射，在实现中，可运用椭圆曲线上 Weil 或 Tate 配对，安全性将依赖于双线性 Diffie-Hellman 问题这一计算难题。

而 Gentry 提出的基于证书的加密模型在生成用户的私钥时需要证书的参与，所以验证过程就具有了保密性。此外，由于用户密钥产生的过程由证书和一个只有用户自己知道的秘密信息共同参与，所以模型中就不存在第三方托管密钥的问题。在基于证书的加密体制（CBE）中不要求发送者获得接收者证书的最新信息，接收者只要公钥通过认证就能够解密消息。

因此，基于无证书的公钥密码体制与基于证书的公钥密码体制从概念上应介于传统公钥密码体制（PKI）和基于身份的公钥密码体制（IBC）之间。Yum 和 Lee 试图在 IBE、CBE 和无证书公钥加密（CL-PKE）之间找到一种正式的等价关系。他们希望基于 IBE 的基础模型给出一种通用的构造，并证明 IBE 可以表示 CBE 和 CL-PKE。为了完成这项工作，他们为 CL-PKE 定义了一个比原始模型安全性较弱的模型。其通用构造方法被许多文献作为完善的构造方法引用。Libert 和 Quisquater 找出了一种利用在原始完整安全模型下 Yum 和 Lee 的将 IBE 转换成 CL-PKE 方案的不安全性。但是他们的攻击不能应用在 Yum 和 Lee 提到的严格安全模型中，所以不能成功地反驳 Yum 和 Lee 的提案。但是随后 Galindo 和 Morillo 则给出了一种有效的攻击方式，指出了 Yum 和 Lee 等的安全问题。

随后 Au 等人提出了另外一种更安全的无证书加密模型。在这个模型中，用户对 KGC 的信任被进一步降低。在 Au 等人的模型中，无证书密码系统的 KGC 可以是被动恶意的。这意味着，KGC 可以是恶意的，因此它可能不会按照 Riyami 等人的设计来产生系统参数和主密钥，但是不主动替换用户的公钥或破坏用户的私钥。因为 KGC 不需要替换用户的公钥或者危害用户的机器来破坏用户的私密密钥，被动恶意的 KGC 会泄露用户的密钥而不会被检测到。在被动恶意的 KGC 模型下，Riyami 等人、Huang 等人和 Li 等人中提出的无证书密码系统都已被证明是不安全的。而 Liu 等人提出的无证书加密方案在 Huang 和 Susilo 等人提出的模型下也是不安全的。而第一个可用的能抵抗被动恶意的 KGC 攻击的唯一被证明是安全的无证书加密方案是由 Libert 和 Quisquater 提出的，但是，它的安全性只在随机预言模型被证明了。之后 Hwang 等人提出了第一个在标准模型下被证明安全的抵抗被动恶意 KGC 攻击的 CL-PKE 方案。

6.2 安全模型

6.2.1 基于无证书的加密模型

最初的无证书密码学的定义有 7 个算法：*Setup*，*Partial-Private-Key-Extract*，*Set-Secret-Value*，*Set-Private-Key*，*Set-Public-Key*，*Encrypt* 和 *Decrypt*。

Setup：算法输入一个安全参数 k 并返回系统的参数 *params* 和主密钥。系统参数包括对消息空间 M 和密文空间 C 的描述。这个算法是被 KGC 来执行的，假设参数是公开的，但是主要密钥只有 KGC 知道。

Partial-Private-Key-Extract：这个算法输入参数 *params*、主要密钥和实体 A 的标识 $ID_A \in \{0,1\}^*$，输出部分私钥 D_A 需要通过安全信道传输给实体 A。

Set-Secret-Value：这个算法将参数 *params* 和 A 的标识 ID_A 作为输入，输出 A 的秘密值 x_A。

Set-Private-Key：这个算法将 *params*，实体 A 的部分私有密钥 D_A 和 A 的秘密值 x_A 作为输入，通过 x_A 将 D_A 转换成完整的私钥 S_A。

Set-Public-Key：这个算法将 *params* 和身份 A 的秘密值 x_A 作为输入，输出实体 A 的公钥 P_A。

Encrypt：这个算法将 *params*，消息 $m \in M$，公有密钥 P_A 和实体 A 的身份 ID_A，返回密文 $c \in C$ 或一个空符号 $\perp$，表明加密失败。

Decrypt：这个算法将 *params*，$c \in C$ 和一个私有密钥 S_A 作为输入，它返回消息 $m \in M$ 或者消息 $\perp$，表明解密失败。

在无证书密码学中通常认为存在以下两种类型的攻击：

Type Ⅰ——密钥替换攻击:第三方在俘获用户私钥并且/或者用第三方选择的某值取代用户公钥后假扮用户。但是第三方不知道用户的部分密钥。

Type Ⅱ——恶意 KGC 攻击:已知用户部分密钥的恶意 KGC 可以假扮用户,然而,KGC 不知道用户的私钥且不能够替换用户的公钥。

6.2.2 Riyami 的安全模型

根据以上的 CL-PKC 定义,Riyami 等人定义了相应的敌手模式。在定义中,有两个参与者分别是敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$。敌手在被给予随机公钥后执行以下 3 个步骤:

步骤 1:$\mathcal{A}$ 可以对其选择的密文进行解密询问,在挑战阶段,$\mathcal{A}$ 选择了两条消息 m_0, m_1,以及通过挑战者对两条消息 m_b 中的一条给予的一个挑战密文 c^*。

步骤 2:$\mathcal{A}$ 做更深入的解密询问,但是不再询问 c^* 的解密。

步骤 3:$\mathcal{A}$ 得到对 b 猜测的结果 b'。定义敌手的优势为

$$Adv(\mathcal{A}) = 2\left(Pr[b' = b] - \frac{1}{2}\right)$$

Riyami 等人扩展了 Boneh 和 Franklin 的模型,使得敌手可以针对他们选择的身份提取出部分私钥或完整私钥或两种都可以。由于方案不采用证书,敌手可以随机选取数值来替换任意实体的公钥,所以需要进一步的加强模型来解决这一问题。同时也需要考虑到针对那些被篡改了公钥的身份,挑战者如何应对密钥提取和解密查询。

以下是敌手为了对抗 CL-PKC 可能的手段及分析:

(1) 提取 A 的部分私钥:$\mathcal{C}$ 通过执行算法 *Partial-Private-Key-Extract* 生成实体 A 的部分私钥 D_A。

(2) 提取 A 的私钥:如 Boneh 和 Franklin 所叙述,允许敌手 $\mathcal{A}$ 对实体的私钥查询,如果 A 的公钥不能被代替,那么 $\mathcal{C}$ 通过算法 *Set-Private-Key* 为实体 A 生成私钥 S_A。

(3) 请求 A 的公钥:当收到对 A 的公钥的第一次请求,$\mathcal{C}$ 通过算法 *Set-Public-Key* 生成实体 A 的公钥 P_A(如果需要 A 先运行 *Set-Secret-Value*),假设公钥对 A 是可用的。

(4) 替换 A 的公钥:$\mathcal{A}$ 可以用 P'_A 反复替换任何实体 A 的公钥 P_A。虽然实施具体的 CL-PKE 方案时,在使用公钥加密之前,可以通过公钥的某种结构来验证公钥的有效性,但这里假设敌手的选择 P'_A 是一个有效的公钥。注意这里任何实体都能很容易地生成有效的公钥。假定 $\mathcal{A}$ 既不能在挑战阶段之前替换挑战的身份 ID_{ch} 的公钥,也不能在某个阶段提取 ID_{ch} 的部分私钥。

(5) 对密文 c 和实体 A 的解密询问:如果 $\mathcal{A}$ 没有替换实体 A 的公钥,那么

$\mathscr{C}$执行 *Set-Private-Key* 获得私钥 S_A，然后输入密文 c 和私钥 S_A 执行 *Decrypt* 算法并将结果返回给 $\mathscr{A}$。但是如果 $\mathscr{A}$ 已经替换了 A 的公钥，由于 $\mathscr{C}$不知道与当前公钥配对的私钥是什么，$\mathscr{C}$不会用与当前公钥相配对的私钥来解密。因此 $\mathscr{C}$对关于 A 的解密询问返回错误。

CL-PKE 的 Type Ⅰ敌手：敌手 $\mathscr{A}_{\mathrm{I}}$ 不能访问主要密钥，但是 $\mathscr{A}_{\mathrm{I}}$ 可以请求任何身份的公钥、部分私钥和完整私钥，并且可以用它选择的值替换公钥，也可以进行解密查询。但也有以下的约束：

（1）在任何时候 $\mathscr{A}_{\mathrm{I}}$ 都不能提取 ID_{ch} 的私钥。

（2）如果任何身份的公钥已经被代替，那么 $\mathscr{A}_{\mathrm{I}}$ 不能请求私钥。

（3）$\mathscr{A}_{\mathrm{I}}$ 既不能在挑战阶段之前代替挑战身份 ID_{ch} 公钥，也不能在任意阶段提取 ID_{ch} 部分私钥。

（4）在第二阶段，$\mathscr{A}_{\mathrm{I}}$ 不能对用身份 ID_{ch} 和公钥 P_{ch} 加密消息 m_b 得到的密文 c^* 进行解密询问。

CL-PKE 的 Type Ⅱ敌手：敌手 $\mathscr{A}_{\mathrm{II}}$ 能够访问主密钥，但是不可以代替实体的公钥。当获得主密钥敌手 $\mathscr{A}_{\mathrm{II}}$ 为它自身计算部分私钥，它也可以对它选择的身份请求公钥，进行私钥查询和解密询问。这种类型的敌手限制如下：

（1）任何时候敌手 $\mathscr{A}_{\mathrm{II}}$ 不能替换公钥。

（2）任何时候敌手 $\mathscr{A}_{\mathrm{II}}$ 不能提取 ID_{ch} 私钥。

（3）在第二阶段，$\mathscr{A}_{\mathrm{II}}$ 不能对用身份 ID_{ch} 和公钥 P_{ch} 加密消息 m_b 得到的密文 c^* 进行解密询问。

CL-PKE 选择密文安全：Riyami 等人定义如果有界多项式敌手 $\mathscr{A}$ 按照以下的规则对抗挑战者的优势是可忽略的，则 CL-PKC 对抗自适应选择密文攻击是语义安全的：

Setup：挑战者选取一个安全参数 k，运行 *Setup* 算法，将系统参数 *params* 返回给 $\mathscr{A}$。如果 $\mathscr{A}$ 是 Type I，那么挑战者自己保留主密钥，否则，他将主密钥给 $\mathscr{A}$。

阶段 1：$\mathscr{A}$ 发起一系列请求，每次请求都是针对某一实体的或是部分私钥查询，或是私钥查询，或是公钥查询，或是公钥替换，或是解密询问。这些询问可能是自适应性的询问，但是受上面定义的规则的限制。

挑战阶段：$\mathscr{A}$ 在阶段 1 结束后，输出一个挑战身份 ID_{ch} 和两个长度相等的明文 $m_0, m_1 \in M$，但 ID_{ch} 不能是在以上查询中使用的身份。而且，如果 $\mathscr{A}$ 属于 Type Ⅰ，那么 ID_{ch} 不能是一个公钥已经被代替且部分私钥被提取的身份。挑战者现在随机选择 $b \in \{0,1\}$，并且计算身份 ID_{ch} 的公钥 P_{ch} 对消息 m_b 加密后的密文 c^*，如果加密的输出是 $\perp$，那么 $\mathscr{A}$ 输掉比赛，否则 c^* 被传递给 m_b。

阶段 2：$\mathscr{A}$ 将再一次发起像阶段 1 那样的一系列请求，但是不允许提取 ID_{ch} 私钥。如果 $\mathscr{A}$ 属于 Type Ⅰ，当 ID_{ch} 的公钥在阶段 1 中已经被替换，则不允许查

询 ID_{ch} 的部分私钥。而且也不允许对 c^* 进行解密查询。

猜想：$\mathcal{A}$ 输出一个猜想 $b' \in \{0,1\}$，如果 $b = b'$ 敌手赢得比赛，定义 $\mathcal{A}$ 在游戏中的优势是 $Adv(\mathcal{A}) := 2\left(Pr[b = b'] - \frac{1}{2}\right)$。

随后，Hu 等人对 Riyami 的方案进行简化，改进后的方案由 5 个多项式时间(PPT)算法组成。在 Hu 等人提出的模型中使用新的无证书方案定义方法比原始使用七个算法的法案更具有通用性，并且新方法保持了无证书方案的特征，那就是用户部分私钥生成和用户密钥生成由 KGC 和用户分别独立地完成。具体来讲，一个具有身份 ID 的用户可以在 KGC 生成用户部分私钥前，生成用户公钥 upk_{ID}。

MasterKeyGen：对于输入为 $1^k, k \in \mathbf{N}$ 并且是一个安全的参数，它产生一个主公/私密钥对 (mpk, msk)。

PartialKeyGen：对于输入为 msk 和用户身份 $ID \in \{0,1\}^*$，它产生一个用户的部分私钥 psk_{ID}。

UserKeyGen：对于输入为 mpk 和用户身份 ID，它产生一个用户的公/私钥对 (upk_{ID}, usk_{ID})。

Encrypt：对于输入为 mpk，用户身份 ID，用户的公钥 upk_{ID} 和消息 m，它返回密文 c。

Decrypt：对于输入为用户的部分密钥 psk_{ID}，用户的私钥 usk_{ID} 以及密文 c，返回明文 m 或者 $\perp$ 表明解密失败。

实现系统时，KGC(密钥产生中心)可能会执行前两个算法：主密钥生成算法和部分密钥生成算法。运行完主密钥生成算法后，主公钥 mpk 可能被公布，并假定系统中的所有人都能够得到它的一个合法副本。KGC 可以通过安全信道发送用户的部分私钥，这样只有预期的用户能够获得它自己的部分密钥。对于用户来说，每个用户要执行用户密钥产生算法来产生它自己的公/私钥对，并公布公钥。

6.2.3 Hu 等人的安全模型

Hu 等人针对两种安全类型，提出了相应的两个敌对模型 $\mathcal{A}_{\mathrm{I}}$ 和 $\mathcal{A}_{\mathrm{II}}$。敌对模型 $\mathcal{A}_{\mathrm{I}}$ 能够破坏用户的私钥 usk_{ID} 或者替换用户的公钥 upk_{ID}，但是不能破坏主私钥 msk，也不能访问用户部分密钥 psk_{ID}。敌手 $\mathcal{A}_{\mathrm{II}}$ 建立了一个恶意却被动的 KGC，它控制生成主公/私钥对，以及控制生成用户的部分密钥 psk_{ID}，在 Huang 和 Wong 的论文中，指定了如下 5 个预言：

CreateUser：输入为一个身份 $ID \in \{0,1\}^*$，如果 ID 没有被创建，预言运行 $psk_{ID} \leftarrow PartialKeygen(msk, ID)$ 和 $(upk_{ID}, usk_{ID}) \leftarrow UserKeyGen(mpk, ID)$。然后存

储(ID,psk_{ID},upk_{ID},usk_{ID})到 *List*,并且创建了 ID,返回 upk_{ID}。

RevealPartialKey:输入为身份 ID,此预言搜索 *List* 寻找 ID 对应的入口。如果没有找到就,返回 $\perp$;否则返回对应的 psk_{ID}。

RevealSecretKey:输入为身份 ID,此预言搜索 *List* 查找 ID 的入口。如果没有找到,返回 $\perp$;否则返回对应的 usk_{ID}。

ReplaceKey:输入为 ID,对应的用户公/私钥对(upk',usk'),此预言搜索 *List* 寻找 ID 的入口。如果没有找到,什么都不会执行。如果 $usk' = \perp$,此预言设置 $usk' = usk_{ID}$。然后,此预言替换 *List* 中的(ID,psk_{ID},upk_{ID},usk_{ID})为(ID,psk_{ID},upk',usk')。

Decryption:输入为身份 ID,密文 c,此预言搜索 *List* 寻找 ID 的入口。如果没有找到,返回 $\perp$。否则,运行 $m \leftarrow Dec(psk_{ID}, usk_{ID}, c)$ 并返回 m。注意原来的 upk_{ID}(由 *CreateUser* 预言返回的)可能会被敌手替换。

在原来的无证书加密敌对模型中,即使在用户公钥被敌手替换后对应的用户私钥是未知的,*Decryption* 预言也应该提供正确的解密。Hu 等人认为此模型可能不现实,并要求 *Decryption* 预言应该使用当前的用户私钥正确地执行解密任务。这当然也包含这样的情况:用户的公钥被敌手替换,但是用户的私钥仍然没有改变。通过使用当前的 usk_{ID} 运行 *Decryption*,从密文恢复出来的消息 m 是 $\perp$ 的可能性也是存在的。

部分密钥替换攻击:在当前可用的所有可比的模型中(Riyami 等人在 2003 年提出的模型,Baek 等人在 2005 年提出的模型,Hu 等人 2006 年和 2007 年提出的模型,Au 等人 2007 年提出的模型等),敌手只可以替换用户的公钥(比如 upk_{ID}),因为在无证书设置中 upk_{ID} 没有经过认证或验证,用户自己产生的公钥在某些公共域上是能被替换的。一个与用户的公钥替换相关更强的攻击场景如下:当用户的随机源已经泄露,这样对应的用户私钥(比如 usk_{ID})就是可知的或者可被敌手控制(比如通过信道攻击 side-channel attackes)。这些敌手的能力已经通过预言 *ReplaceKey* 和 *RevealSecretKey* 来捕获。在实际的应用中用户的部分密钥 psk_{ID} 需要被重新产生。比如,用户丢失他以前的用户部分密钥。在另一个例子中,恶意却被动的 KGC 在知道特定用户的公钥后,可能想要尝试不同的值来猜测出用户的部分密钥,从而导致用户的秘密被泄露。在这种情况中,KGC 可能发送给用户一个指定的部分密钥,当与用户的私钥结合时,可能会泄露信息,导致 KGC 解密用户密文的机会增加。要注意的是,替换用户的部分密钥(*ReplacePartialKey*)和泄露用户的部分密钥(*RevealPartialKey*)之间的区别是前者是自适应的,而后者是静态的。

在 Dent 等人在 2007 年提出了一个对于访问 Type Ⅱ 敌对的解密预言的变种,叫做 *Weak PPK Decrypt*。这个预言输入不仅需要 ID 和密文 c,还需要用户临

时部分密钥 psk'_{ID}。解密密文 c 是通过使用当前的用户私钥 usk_{ID} 和这个临时的用户部分密钥 psk'_{ID}，而不是当前的用户部分密钥 psk_{ID}。事实上，通过 *Weak PPK Decrypt* 发起的新攻击与通过 *ReplaceParticalKey* 发起的是等价的。一方面，*ReplaceParticalKey* 能够包含 *Weak PPK Decrypt*，对于 *Weak PPK Decrypt* 的询问可以通过一系列的询问包括 *ReplaceParticalKey* 和 *Decryption* 来替换。首先，将 psk_{ID} 变成 psk'_{ID} 时 *ReplaceParticalKey* 会被询问。接着为了解密密文 c，*Decryption* 也会被询问，最后为了恢复原来的用户部分密钥 psk_{ID}，*ReplaceParticalKey* 还会被询问。如果 psk_{ID} 还不知道，*RevealParticalKey* 会被首先询问。另一方面，*Weak PPK Decrypt* 也能包含 *ReplaceParticalKey*，*ReplaceParticalKey* 并不影响挑战密文 c^* 的产生（从 m_0 或 m_1 中产生）。同样，*ReplaceParticalKey* 必须得和 *Decryption* 一起使用来返回信息给敌手。这两个询问由 *Weak PPK Decrypt* 一次询问完成。下面是完整的 *ReplaceParticalKey* 预言的描述。

ReplaceParticalKey：输入为一个身份 *ID* 和用户部分密钥 *psk'*，此预言搜索 *List* 寻找 *ID* 的入口，如果没有找到，什么都不执行。如果找到，更新 $(ID, psk_{ID}, upk_{ID}, usk_{ID})$ 为 $(ID, psk'_{ID}, upk_{ID}, usk_{ID})$。

Dent 等人说明一旦被允许访问 *Weak PPK Decrypt* 预言，则这个 CLE 方案在被动恶意 KGC 安全的 CLE 方案的攻击下就不再安全了。由于 *Weak PPK Decrypt* 与 *ReplaceParticalKey* 在游戏中产生相同的效果，这个例子还阐明了恶意 KGC Type Ⅱ安全 CLE 方案可能不安全，如果对于被允许 *ReplaceParticalKey*。

通过以下两个游戏对两种类型的安全模型进行详细说明：

Game Ⅰ：$\mathscr{C}_{\mathrm{I}}$ 是挑战者/模拟者，$k \in \mathbf{N}$ 是安全参数：

（1）$\mathscr{C}_{\mathrm{I}}$ 运行 $(mpk, msk) \leftarrow MasterKeyGen(1^k)$，接着输入 1^k 和 mpk 激活 $\mathscr{A}_{\mathrm{I}}$。

（2）$\mathscr{A}_{\mathrm{I}}$ 可以查询 *CreateUser*，*RevealPartialKey*，*RevealSecretKey*，*ReplaceKey*，*ReplacePartialKey* 和 *Decryption*。最后，$\mathscr{A}_{\mathrm{I}}$ 提交两个长度相等的消息 (m_0, m_1)，同时还有目标身份 ID^*。

（3）$\mathscr{C}_{\mathrm{I}}$ 选择一个随机位 $b \in \{0,1\}$，通过运行 $c^* \leftarrow Enc(mpk, ID^*, upk_{ID^*}, m_b)$ 计算挑战密文 c^*，并将 c^* 返回给 $\mathscr{A}_{\mathrm{I}}$，upk_{ID^*} 是当前在 *List* 中对应 ID^* 的用户公钥。

（4）$\mathscr{A}_{\mathrm{I}}$ 继续按照第 2 步查询。最后，会输出 b'。

$\mathscr{A}_{\mathrm{I}}$ 赢得比赛，如果 $b' = b$，并且 $\mathscr{A}_{\mathrm{I}}$ 既没有查询关于 ID^* 的 *RevealPartialKey*，也没有查询关于 ID^* 的 *ReplacePartialKey*；$\mathscr{A}_{\mathrm{I}}$ 没有查询关于 (ID^*, c^*) 的 *Decryption*。用 $Pr[\mathscr{A}_{\mathrm{I}}\ Succ]$ 表示 $\mathscr{A}_{\mathrm{I}}$ 赢得比赛的可能性，并用 $Adv_{\mathscr{A}_{\mathrm{I}}} = \left| Pr[\mathscr{A}_{\mathrm{I}}\ Succ] - \frac{1}{2} \right|$ 定义 $\mathscr{A}_{\mathrm{I}}$ 在 *Game* Ⅰ中的优势。

Game Ⅱ：$\mathscr{C}_2$ 是模拟者/挑战者，$k \in \mathbf{N}$，是安全参数。

(1) $\mathscr{C}_2$ 输入 k 比特参数执行 $\mathscr{A}_{\text{II}}$,并获得主公钥 mpk。

(2) $\mathscr{A}_{\text{II}}$ 之后可以开始查询 *CreateUser*, *RevealSecretKey*, *ReplaceKey*, *ReplacePartialKey* 和 *Decryption*。注意语言 *RevealSecretKey* 将不再需要,因为 $\mathscr{A}_{\text{II}}$ 可能知道主私钥 msk。或者 $\mathscr{A}_{\text{II}}$ 在产生 mpk 时可能没有按照 *MasterKeyGen* 的说明。同样也要注意到,当 $\mathscr{A}_{\text{II}}$ 查询 *CreateUser*,它必须同时提供用户的部分密钥 psk_{ID}。在这一步的最后,$\mathscr{A}_{\text{II}}$ 提交两个等长消息(m_0, m_1),还有目标身份 ID^*。

(3) $\mathscr{C}_{\text{II}}$ 随机地选择一个位 b,并运行 $c^* \leftarrow Enc(mpk, ID^*, upk_{ID^*}, m_b)$,计算挑战密文 c^*,并将 c^* 返回给 $\mathscr{A}_{\text{II}}$。

(4) $\mathscr{A}_{\text{II}}$ 继续按照第 2 步提供查询。最后,会输出 b'。

$\mathscr{A}_{\text{II}}$ 赢得比赛,如果 $b' = b$,并且:① $\mathscr{A}_{\text{II}}$ 没有查询关于 ID^* 的 *RevealSecretKey*;② $\mathscr{A}_{\text{II}}$ 没有查询关于$(ID^*, \cdot, \cdot)$的 *ReplaceKey* 来替换 upk_{ID^*};③ $\mathscr{A}_{\text{II}}$ 没有查询关于(ID^*, c^*)的 *Decryption*。相似地,用 $Pr[\mathscr{A}_{\text{II}}\ Succ]$ 表示 $\mathscr{A}_{\text{II}}$ 赢得比赛的可能性,并用 $Adv_{\mathscr{A}_{\text{II}}} = \left| Pr[\mathscr{A}_{\text{II}}\ Succ] - \frac{1}{2} \right|$ 定义 $\mathscr{A}_{\text{II}}$ 在 *Game* II 中的优势。要注意的是,上面的游戏捕捉恶意却被动的 KGC 攻击,因为 mpk 是由敌手 $\mathscr{A}_{\text{II}}$ 来产生的,而不是由游戏的挑战者 $\mathscr{C}_{\text{II}}$ 产生的。

定义 无证书加密方案 CLE 是 Type I IND-ID-CCA2 安全的(Type II IND-ID-CCA2 安全的),如果不存在可能的多项式时间的敌手 $\mathscr{A}_{\text{I}}$($\mathscr{A}_{\text{II}}$)来以不可忽视的优势赢得 *Game* I(*Game* II)。CLE 被称为是 IND-ID-CCA2 安全的,如果既是 Type I IND-ID-CCA2 安全的又是 Type II IND-ID-CCA2 安全的。

6.3 Riyami 的加密方案

Riyami 的 CL-PKC 工作很大程度上是基于 Boneh 和 Franklin 的 ID-PKC 工作展开的。

Setup:

(1) 输入 k,输出$\langle G_1, G_2, e\rangle$,其中 G_1 和 G_2 是素数 q 阶群,$e: G_1 \times G_1 \rightarrow G_2$ 是配对函数。

(2) 随机选择 $P \in G_1$。

(3) 随机从 Z_q^* 中选择一个主密钥 s,令 $P_0 = sP$。

(4) 选择 Hash 函数 $H_1: \{0,1\}^* \rightarrow G_1^*$, $H_2: G_2 \rightarrow \{0,1\}^*$, $H_3: \{0,1\}^n \times \{0,1\}^n \rightarrow Z_q^*$ 和 $H_4: \{0,1\}^n \rightarrow \{0,1\}^n$,这里 n 是明文的位长。

系统参数 $params = \langle G_1, G_2, e, n, P, P_0, H_1, H_2, H_3, H_4\rangle$。主密钥是 $s \in Z_q^*$,消息空间 $M = \{0,1\}^n$,密文空间 $C = G_1 \times \{0,1\}^{2n}$。

Partial-Private-Key-Extract:输入身份 $ID_A \in \{0,1\}^*$,按以下步骤为身份 ID_A 的实体 A 构建部分私钥:

(1) 计算 $Q_A = H_1(ID_A) \in G_1^*$。

(2) 输出部分私钥 $D_A = sQ_A \in G_1^*$。

Set-Secret-Value:将 *params* 和实体身份 ID_A 作为输入,随机选择 $x_A \in Z_q^*$,x_A 作为 A 的秘密值。

Set-Private-Key:将 *params*、实体 A 的部分私钥 D_A 和 A 的秘密值 $x_A \in Z_q^*$ 作为输入,计算私钥 $s_A = x_A D_A = x_A sQ_A \in G_1^*$。

Set-Public-Key:将 *params*、实体 A 的秘密值 $x_A \in Z_q^*$ 作为输入,构造 A 的公钥 $P_A = \langle X_A, Y_A \rangle$,其中 $X_A = x_A P, Y_A = x_A P_0 = x_A sP$。

Encrypt:用公钥 $P_A = \langle X_A, Y_A \rangle$ 和实体 A 的身份 $ID_A \in \{0,1\}^*$ 对消息 $m \in M$ 进行加密:

(1) 检查 $X_A, Y_A \in G_1^*$ 是否满足 $e(X_A, P_0) = e(Y_A, P)$,如果不满足,输出 $\perp$ 并终止加密。

(2) 计算 $Q_A = H_1(ID_A) \in G_1^*$。

(3) 随机选择 $\sigma \in \{0,1\}^n$。

(4) $r = H_3(\sigma, m)$。

(5) 计算并输出密文:$c = \langle rP, \sigma \oplus H_2(e(Q_A, Y_A)^r, m \oplus H_4(\sigma)) \rangle$。

Decryt:假设 $c = \langle U, V, W \rangle \in C$,用私钥 S_A 解密密文:

(1) 计算 $V \oplus H_2(e(S_A, U)) = \sigma'$。

(2) 计算 $W \oplus H_4(\sigma') = m'$。

(3) 设 $r' = H_3(\sigma', m')$,测试是否 $U = r'P$,如果不是,输出 $\perp$ 然后拒绝密文。

(4) 输出 m' 作为 c 的解密。

如果 c 是 P_A 和 ID_A 对 m 加密后的有效密文,易得 $m' = m$。其中 W 可以被 $W = E_{H_4(\sigma)}(m)$ 代替,E 表示语义安全的对称加密方案。

对于 CL-PKE 方案的安全分析 Riyami 等人给出了如下定理:

定理 6.1 设 Hash 函数 H_1, H_2, H_3 和 H_4 是随机预言。如果没有多项式有界算法存在不可忽略的优势解决 GBDHP 问题,那么 CL-PKE 是 IND-CCA 安全的。

6.4 Yum 和 Lee 的方案及分析

Yum 和 Lee 等人提出了基于公有密钥加密和基于身份加密的无证书加密的通用安全结构。设 $\Pi_{ID} = (ID.Gen, ID.Ext, ID.Enc, ID.Dec)$ 是一个安全的基于

身份加密的方案，为了避免 Π_{ID} 密钥托管的问题，Yum 等人采用双解密的想法。安全无证书加密方案 $\psi_{CL}=(CL.Gen, CL.PartialKey, CL.SecretVal, CL.SetPrivKey, CL.SetPubKey, CL.Enc, CL.Dec)$ 可以构建如下：

$CL.Gen(1^k)$
$(ID.pms_{KGC}, ID.msk_{KGC}) \leftarrow ID.Gen(1^k)$
$CL.msk \leftarrow ID.msk_{KGC}$
$CL.pms \leftarrow ID.pms_{KGC}$
Return $(CL.pms, CL.msk)$

$CL.PartialKey(CL.pms, CL.msk, ID_A)$
$d_A \leftarrow ID.Ext(CL.pms, CL.msk, ID_A)$
$D_A \leftarrow (d_A, ID_A)$
Return D_A

$CL.SecretVal(CL.pms, ID_A)$
$(ID.pms_A, ID.msk_A) \leftarrow ID.Gen(1^k)$
$x_A \leftarrow (ID.pms_A, ID.msk_A, ID_A)$
Return x_A

$CL.SetPrivKey(CL.pms, D_A, x_A)$
Parse x_A as $(ID.pms_A, ID.msk_A, ID_A)$
Parse D_A as (d_A, ID_A)
$d'_A \leftarrow ID.Ext(ID.pms_A, ID.msk_A, ID_A)$
$S_A \leftarrow (d_A, d'_A, ID.pms_A)$
$S_A \leftarrow (d_A, d'_A, ID.pms_A)$
Return S_A

$CL.SetPubKey(CL.pms, x_A)$
Parse x_A as $(ID.pms_A, ID.msk_A, ID_A)$
$P_A \leftarrow ID.pms_A$
Return P_A

$CL.Enc(CL.pms, m, P_A, ID_A)$
$c' \leftarrow ID.Enc(P_A, ID_A, m)$
$c \leftarrow ID.Enc(CL.pms, ID_A, c')$
Return c

$CL.Dec(CL.pms, S_A, c)$
Parse S_A as $(d_A, d'_A, ID.pms_A)$
$c' \leftarrow ID.Dec(CL.pms, d_A, c)$
$m \leftarrow ID.Dec(ID.pms_A, d'_A, c')$
Return m

但是 Galindo 和 Morillo 指出 Yum 等人的通用构造遇到了在基于证书的加密机制中同样的问题，不能抵御 CL-PKC Type Ⅱ的敌手的攻击：

（1）挑战者将 KGC 的主密钥 $CB.msk$ 传递给 CL-PKC Type Ⅱ的敌手 $\mathcal{A}_{Ⅱ}$，敌手可以通过运行 $D_A^* \leftarrow CL.PartialKey(CL.pms, CL.msk, ID_A^*)$ 为用户 ID_A^* 生成部分私钥 $D_A^* = (d_A^*, ID_A^*)$。

（2）利用部分私钥解密并获得 $c' \leftarrow ID.Dec(CL.pms, d_A^*, c^*)$。

（3）由于 $ID.Enc$ 是概率算法，则 $\mathcal{A}_{Ⅱ}$ 对 c' 重新加密，直到获得 $c'' = ID.Enc(P_A^*, ID_A^*, c')$，其中 $c'' \neq c^*$。

（4）$\mathcal{A}_{Ⅱ}$ 为 c'' 生成解密预言。由于 $c'' \neq c^*$，是可以解密查询的，从而 $\mathcal{A}_{Ⅱ}$ 重新得到消息 m_b。

Galindo 和 Morillo 指出通过以上步骤 $\mathcal{A}_{Ⅱ}$ 存在 1/2 的优势可以说明，Yum 等人的方案对于来自密钥生成中心的自适应选择密文攻击是不具有安全性的。

6.5 被动恶意 KGC 攻击

针对 Type Ⅱ攻击的防范措施关键就是要解决密钥托管问题。也就是说即使 KGC 是恶意的，在已知用户的部分密钥但 KGC 不会主动地替换用户公钥（现实中公钥会发布在电子公告板上）或者损坏用户的私密密钥的情况下，KGC 也不能以用户的身份执行任何加密操作。此外，即使说 KGC 是恶意的，也是假设在被动的前提下。恶意的 KGC 可能被动地窃听发送给用户的密文并试图利用他掌握的用户部分密钥破解密文。

如果 KGC 是主动的，那么 KGC 不但掌握用户的部分密钥而且有能力替换用户的公钥或者获得用户的私钥，则 KGC 总是能够假扮用户。在 PKI 中也有同样的情况发生。一个恶意而且主动的 CA（认证权威）可以通过生成伪造的证书假扮用户对用户进行同样的破坏。通过对之前的无证书加密的比较，Au 等人的目的不是减弱对 KGC 的信任，而是要减轻恶意但是被动的 KGC 的破坏。

回顾所有 2007 年前提出的无证书加密、签名方案和对抗模型，就会注意到所有的这些都假设被动恶意的 KGC 总是诚实地按照方案的规定生成了公/私钥对。也就是说所有这些都假设 KGC 正常地初始化。但是可以在 KGC 设置自己的密钥对后就突然变得恶意而且准备伪装攻击用户。这样 KGC 可以获得用户的私钥，这个恶意生成的主公钥与 KGC 按照方案中规定的方式诚实地生成的主公钥在计算上是很难区分的。这就意味着一旦去掉 KGC 必须按规定生成它的主密钥对这个假设条件，关于密钥托管的问题就会在先前提出的一些无证书方案中再次出现。

Au 等人设计了新的 Type Ⅱ对抗模型，来解决恶意但被动的 KGC 攻击。新的模型去掉了 KGC 必须在主密钥生成阶段和运行用户部分私钥生成阶段才能开始运行的假设。新模型也允许 KGC 在主密钥生成阶段选择一个用户来攻击。Au 采用简化定义的理念并加强由 Hu，Wong，Zhang 和 Deng 提出的无证书签名方案的对抗模型。

无证书加密系统由 5 个多项式时间算法组成：*MasterKeyGen*，*PartialKeyGen*，*UserKeyGen*，*CL-Encrypt* 和 *CL-Decrypt*。

MasterKeyGen：输入 1^k 其中 $k \in \mathbf{N}$，是一个安全参数，它生成一个主公/私钥对（mpk，msk）。设 $MPK(k)$ 为所有通过 MasterKeyGen（1^k）算法产生的主公钥集合。在不失一般性的条件下，假设一个主公钥 mpk 是否属于 $MPK(k)$ 是可计算的。

PartialKeyGen：输入 mpk 和用户身份 $ID \in \{0,1\}^*$，算法产生一个用户部分密钥 *partial_key*。

UserKeyGen：输入 mpk 和用户身份 ID，算法输出一个用户公/私钥对（upk，usk）。

CL-Encrypt：输入 mpk，用户身份 ID，用户公钥 upk，消息 m，算法返回一个密文 c。

CL-Decrypt：输入用户私密密钥 usk，用户部分密钥 *partial_key* 和密文 c，算法返回一条消息 m。

对于所有的 $k \in \mathbf{N}$，$m \in \{0,1\}^*$，$ID \in \{0,1\}^*$，如果（mpk，msk）$\leftarrow MasterKeyGen(1^k)$，$c_0^* = m_b \cdot X_{ID^*}^c$，$c_2^* = c_1^{*U_{ID^*}} = (g^c)^{U_{ID^*}}$，$c_3^* = c_1^{*K(w^*)}$，（$upk$，$usk$）$\leftarrow UserKeyGen(mpk, ID)$，可得 $m \leftarrow CL\text{-}Decrypt(usk, partial\_key, CL-Encrypt(mpk, ID, upk, m))$。令 $partial\_key_{ID}$ 代表 ID 用户的部分私钥，其公/私钥对表示为（upk_{ID}，usk_{ID}）。

定义两种类型的敌手 $\mathcal{B}_{\mathrm{I}}$ 和 $\mathcal{B}_{\mathrm{II}}$。敌手 $\mathcal{B}_{\mathrm{I}}$ 模拟第三方开始密钥替换攻击。$\mathcal{B}_{\mathrm{II}}$ 通过恶意而被动的 KGC 来开展攻击。五种可以被敌手访问的预言为：*CreateUser*，*RevealPartialKey*，*RevealSecretKey*，*ReplaceKey* 和 *Decrypt*。

CreateUser：输入身份 $ID \in \{0,1\}^*$，如果 ID 已经被创建，则什么也不执行，否则，预言生成 $partial\_key_{ID} \leftarrow PartialKeyGen(msk, ID)$，$(upk_{ID}, usk_{ID}) \leftarrow UserKeyGen(mpk, ID)$。这种情况下，$ID$ 就被创建了。在两种情况中都将返回 upk_{ID}。

RevealPartialKey：输入身份 ID，如果 ID 被创建，返回 $partial\_key_{ID}$。否则，返回符号 $\perp$。

RevealSecretKey：输入身份 ID，如果 ID 已经被创建，返回相对应用户的私密密钥 usk_{ID}，否则返回符号 $\perp$。

ReplaceKey:输入身份 *ID* 和用户公/私钥对(upk^*,usk^*),如果 *ID* 已经被创建,(upk^*,usk^*)代替用户原始的公/私钥对。否则,不执行任何操作。

Decrypt:输入身份 *ID* 和密文 c,解密预言为以下三种情况之一:

(1) 如果 *ID* 没有被创建并且密钥对(upk_{ID},usk_{ID})没有被替换,则将会返回消息 m,其中:$m \leftarrow CL\text{-}Decrypt(usk_{ID}, partial\_key_{ID}, c)$。

(2) 如果 *ID* 没有被创建,则返回符号 $\perp$。

(3) 如果用户 *ID* 的公/私钥对被(upk^*,usk^*)替换,则预言返回 m 形式如下:$m \leftarrow CL\text{-}Decrypt(usk^*, partial\_key_{ID}, c)$,其中 $m \neq \perp$。如果 $m = \perp$,则预言运行一个特殊的"知识生成器"来解密密文 c,并且将消息返回给敌手。注意,每一个 CL-ENC 方案的知识生成器的构建都是不一样的。

Type Ⅰ:设 $\mathscr{C}_{\mathrm{I}}$ 为挑战者,$k \in \mathbf{N}$ 是安全参数,则

(1) $\mathscr{C}_{\mathrm{I}}$ 运行 $MasterKeyGen(1^k)$ 来获取(mpk,msk)。

(2) $\mathscr{C}_{\mathrm{I}}$ 针对 1^k 和 mpk 运行 $\mathscr{B}_{\mathrm{I}}$ 类型攻击,在模拟过程中,$\mathscr{B}_{\mathrm{I}}$ 能产生 *CreateUser*, *RevealPartialKey*, *RevealSecretKey*, *ReplaceKey* 和 *Decrypt* 查询。最后,$\mathscr{B}_{\mathrm{I}}$ 输出两个等长的消息(m_0,m_1)和一个目标身份 ID^*。

(3) $\mathscr{C}_{\mathrm{I}}$ 随机选择 $b \in \{0,1\}$,然后给出挑战密文 c^* 传送给 $\mathscr{B}_{\mathrm{I}}$,其中:$c^* \leftarrow CL\text{-}Encrypt(mpk, ID^*, upk_{ID^*}, m_b)$。

(4) $\mathscr{B}_{\mathrm{I}}$ 按照步骤 2 生成查询。最后,$\mathscr{B}_{\mathrm{I}}$ 输出一个推测 $b' \in \{0,1\}$。如果 $b' = b$ 则 $\mathscr{B}_{\mathrm{I}}$ 攻击成功,限制条件为:① $\mathscr{B}_{\mathrm{I}}$ 从未使用 $RevealPartialKey(ID^*)$ 查询来获得 $partial\_key_{ID^*}$;② $\mathscr{B}_{\mathrm{I}}$ 从未查询过(ID^*,c^*)的 Decrypt 预言。

如果对于所有的 $\mathscr{B}_{\mathrm{I}}$ 中的概率多项式时间算法对于 $\mathscr{A}_{\mathrm{I}}$ 取得攻击的成功都是可忽略的,则认为 CL-ENC 方案在 Type Ⅰ中是安全的。

注:$\mathscr{B}_{\mathrm{I}}$ 可以在身份 *ID* 的密钥替换查询产生之前来进行 *RevealSecretKey*(ID^*)查询。目前,针对 Type Ⅱ攻击模型中,以前的所有模型均没有考虑到敌手具有这种能力。在以前的模型中,尽管敌手 $\mathscr{B}_{\mathrm{I}}$ 能够替换用户的公/私钥对,但是敌手不能够重新获得原始用户利用身份 ID^* 生成的私密密钥。

Type Ⅱ:设 $\mathscr{C}_{\mathrm{II}}$ 为挑战者,$k \in \mathbf{N}$ 是安全参数,则

(1) $\mathscr{C}_{\mathrm{II}}$ 针对 1^k 和特殊 *master-key-gen* 运行 $\mathscr{B}_{\mathrm{II}}$ 类型的攻击。$\mathscr{B}_{\mathrm{II}}$ 返回一个主公钥 $mpk \in MPK(k)$。

(2) $\mathscr{B}_{\mathrm{II}}$ 进行 *RevealSecretKey*, *ReplaceKey* 和 *Decrypt* 预言查询。$\mathscr{B}_{\mathrm{II}}$ 同样可以进行攻击签名Ⅱ中描述的 *CreatUser* 预言查询。最后,$\mathscr{B}_{\mathrm{II}}$ 输出两个等长的消息(m_0,m_1)和一个目标身份 ID^*。

(3) $\mathscr{C}_{\mathrm{II}}$ 随机选择 $b \in \{0,1\}$ 并且将密文 c^* 和一个标签 *guess* 作为输入值传递给 $\mathscr{B}_{\mathrm{II}}$,其中 $c^* \leftarrow CL\text{-}Encrypt(mpk, ID^*, upk_{ID^*}, m_b)$,运行 $\mathscr{B}_{\mathrm{II}}$。

(4) $\mathcal{B}_{\text{II}}$ 生成步骤 2 中描述的查询，最后，$\mathcal{B}_{\text{II}}$ 输出一个推测值 $b' \in \{0,1\}$。如果 $b'=b$，则 $\mathcal{B}_{\text{II}}$ 攻击取得成功，限制条件为：$\mathcal{B}_{\text{II}}$ 从未查询过 *RevealSecretKey*(ID^*) 来获取用户的私密密钥 usk_{ID^*}；$\mathcal{B}_{\text{II}}$ 在收到 c^* 之前从未查询过 *ReplaceKey*(ID^*，·，·)；$\mathcal{B}_{\text{II}}$ 从未对(ID^*，c^*)进行过 *Decrypt* 查询。

如果对于所有的 $\mathcal{B}_{\text{II}}$ 中的概率多项式时间算法对于 $\mathcal{B}_{\text{II}}$ 取得攻击的成功都是可以忽略的，则认为 CL-ENC 方案在 Type Ⅱ中是安全的。

以前对于对抗模型 Type Ⅱ中敌手不能替换系统中任意用户的公钥，在上面的 Type Ⅱ中，Au 等人放松了对此条件约束，允许敌人在对应 ID^* 的用户公钥在收到 c^* 之前没有被替换的条件下执行 *ReplaceKey*，同样允许在收到 c^* 后替换 ID^* 身份对应的用户公钥。

6.6 Au 等人对 Riyami 方案分析

Au 等人对 Riyami 等人提出的方案进行了分析，证明 Riyami 等人提出的方案对于恶意但被动的 KGC 攻击是脆弱的。需要注意的是，这个攻击不是在 Riyami 提出的原始安全模型中进行的，而是在 Hu 等人提出的模型中进行的。

为了获取任意被选定身份 ID^* 的用户的私密密钥，KGC 随机选择 $\alpha \in_R Z_q$ 并计算 $g=H(ID^*)^{\alpha}$，之后执行算法 *MasterKeyGen* 和 *PartialKeyGen*。

假设身份为 ID^* 的公钥被公布为($X_{ID^*}=g^x$，$Y_{ID^*}=g^{\alpha x^*}$)，其中 $x^* \in_R Z_q$。通过用户的公钥，KGC 能计算出用户的私密密钥 $usk_{ID^*}=Y_{ID}^{\alpha^{-1}}$。由于用户的部分密钥由 KGC 生成，在获取了受害用户的私密密钥后，KGC 可以解密受害用户加密的密文以及代表受害用户生成其对应的签名。

同时 Au 等人也指出很多其他使用了与 Riyami 等人相同的密钥结构无证书加密系统对于这种攻击同样具有脆弱性。

但 Au 指出，Libert 和 Quisquater 提出的无证书加密的构建方案，具有抵抗选择密文攻击的安全性。他们提出的方案是以传统的公钥加密和基于身份的加密为基础的。用 $\Pi^{PKE}=(K^{PKE},\varepsilon^{PKE},D^{PKE})$ 和 $\Pi^{IBE}=(Setup^{IBE},Extract^{IBE},\varepsilon^{IBE},D^{IBE})$ 来分别表示一个 PKE 方案和一个 IBE 方案。

MasterKeyGen：运行 $Setup^{IBE}(1^k)$ 来生成(mpk^{IBE}，msk^{IBE})并设置主公/私钥对(mpk，msk) := (mpk^{IBE}，msk^{IBE})。

PartialKeyGen：运行 $usk^{IBE} \leftarrow Extract^{IBE}(msk^{IBE}, ID)$ 并设置 $partial\_key_{ID} := usk^{IBE}$。

UserKeyGen：运行(upk^{PKE}，usk^{PKE})$\leftarrow K^{PKE}(1^k)$并设置(upk_{ID}，usk_{ID}) := (upk^{PKE}，usk^{PKE})。消息空间定义为关于 upk^{PKE} 的 Π^{PKE} 的消息空间。要求对应于 upk^{PKE} 的

Π^{PKE} 密文空间是关于 mpk 的 Π^{IBE} 的消息空间的子集。

CL-Encrypt:用身份 ID 和 upk_{ID} 加密消息 m,算法计算如下:$c = \varepsilon^{IBE}(mpk, ID, \varepsilon^{IBE}(upk_{ID}, m))$。

CL-Decrypt:解密密文 c,算法计算过程如下:

(1) $m \leftarrow D^{IBE}(partial\_key_{ID}, ID, c)$,如果 $m = \perp$,则输出 $\perp$,并终止运行。

(2) 否则,计算 $m' \leftarrow D^{PKE}(usk_{ID}, m)$,并输出 m'。

该方案已经被证明在 Π^{PKE} 和 Π^{IBE} 条件下是具有 CPA(chosen plaintext attack)语义安全的。接下来的定理表明在新模型中该方案同样具有 CPA 安全。

定理 6.2 上文中的方案在第 2 部分定义的 Type Ⅰ和 Type Ⅱ中不能够访问解密预言,并且 Π^{PKE} 和 Π^{IBE} 具有 CPA 安全性。

证明:在不允许反问解密预言 *Decrypt* 条件下,Type Ⅰ和 Type Ⅱ仅提供 CPA 安全。

首先说明下一个攻击者 $\mathscr{C}_{\mathrm{I}}$ 如何利用一个敌手 $\mathscr{B}_{\mathrm{I}}$ 来破坏 Π^{IBE} 的 CPA 安全性。$\mathscr{C}_{\mathrm{I}}$ 从模拟者 S^{IBE} 处获得基于身份的主公共密钥 mpk^{IBE},并将 mpk^{IBE} 当做 mpk 传送给 $\mathscr{B}_{\mathrm{I}}$。在 $\mathscr{C}_{\mathrm{I}}$ 与 $\mathscr{B}_{\mathrm{I}}$ 的通信中,用 ID_i 来表示 $\mathscr{B}_{\mathrm{I}}$ 产生查询中的第 i 个不同的身份。设 q_{ID} 为包括在所有查询中的不同身份的数目。$\mathscr{C}_{\mathrm{I}}$ 随机选择一个数 $l \in_R \{1, \cdots, q_{ID}\}$。$\mathscr{C}_{\mathrm{I}}$ 模拟如下的预测过程:

CreatUser:输入 ID_i,$\mathscr{C}_{\mathrm{I}}$ 运行 K^{PKE} 来产生用户公/私钥对 $(upk_i^{PKE}, usk_i^{PKE})$。如果 $i \neq l$,$\mathscr{C}_{\mathrm{I}}$ 对 ID_i 的用户部分私钥 usk_i^{IBE} 进行 S^{IBE} 查询,否则设置 usk_i^{IBE} 为 $\perp$。$\mathscr{C}_{\mathrm{I}}$ 将 $(ID_i, usk_i^{PKE}, upk_i^{PKE}, usk_i^{IBE})$ 存储在它的数据库中,并且返回 upk_i^{PKE}。

RevealPartialKey:输入 ID_i,如果 $i = l$,$\mathscr{C}_{\mathrm{I}}$ 终止运行,否则在它的数据库中查找 ID_i 用户的部分密钥 usk_i^{IBE},如果查询到则将其返回给 $\mathscr{B}_{\mathrm{I}}$,否则返回 $\perp$。

RevealSecretKey:输入 ID_i,如果存在,$\mathscr{C}_{\mathrm{I}}$ 返回 usk_i^{PKE},否则返回 $\perp$。

ReplaceKey:输入 ID_i 和 (upk^*, usk^*),如果 ID_i 已经被创建,则 $\mathscr{C}_{\mathrm{I}}$ 利用 upk^* 替换 ID_i 的公钥,利用 usk^* 替换用户 ID_i 的私密密钥。否则不进行任何操作。注意,usk^* 不可以为空字符串。

在攻击阶段,$\mathscr{B}_{\mathrm{I}}$ 输出两个等长的消息 (m_0, m_1) 和一个目标身份 ID^*。如果 $ID^* \neq ID_l$,则 $\mathscr{C}_{\mathrm{I}}$ 终止运行。否则,将 m_0, m_1 分别加密成 $c_0 = \varepsilon^{PKE}(upk_l^{PKE}, m_0)$ 和 $c_1 = \varepsilon^{PKE}(upk_l^{PKE}, m_1)$,再将它们与目标身份 ID_l 作为攻击请求传送给 S^{IBE}。由 S^{IBE} 准备的攻击 $c^* = \varepsilon^{IBE}(mpk, ID_l, c_b)$,$b \in_R \{0,1\}$ 转发给 $\mathscr{B}_{\mathrm{I}}$。

将 $\mathscr{C}_{\mathrm{I}}$ 对 S^{IBE} 中隐藏的比特 b 的推测输出作为 $\mathscr{B}_{\mathrm{I}}$ 的输出 $b' \in \{0,1\}$。如果 $\mathscr{B}_{\mathrm{I}}$ 成功,则 $\mathscr{C}_{\mathrm{I}}$ 同样取得成功。后者对于 $\mathscr{B}_{\mathrm{I}}$ 攻击的身份的推测成功率至少为 $1/q_{ID}$。同样需要注意的是这种情况中 $ID^* = ID_l$,$\mathscr{B}_{\mathrm{I}}$ 不允许对 ID_l 进行 *RevealPartialKey* 查询,因此,模拟在这种情况下不会终止。

下面说明该方案在 Type Ⅱ攻击中具有 CPA 安全性(特别地,可以抵御恶意但被动的 KGC 攻击)。描述 $\mathscr{C}_{Ⅱ}$ 如何利用敌人 $\mathscr{B}_{Ⅱ}$ 来破坏 Π^{PKE} 的 CPA 安全性。在 Type Ⅱ的第一步中,$\mathscr{B}_{Ⅱ}$ 被运行并且 $\mathscr{B}_{Ⅱ}$ 返回一个主公钥 mpk。注意 $\mathscr{B}_{Ⅱ}$ 没有利用执行 $Setup^{IBE}$ 来产生 mpk。$\mathscr{C}_{Ⅱ}$ 随机选择一个序号 $l \in_R \{1,\cdots,q_{ID}\}$,其中 q_{ID} 是包括在查询中所有不同身份的数目,从模拟者 S^{PKE} 获得一个攻击公钥 pk^*,$\mathscr{C}_{Ⅱ}$ 模拟过程如下:

CreatUser:输入 ID_i 和 $partial\_key_i$,如果 $i=l$,设 $upk_i^{PKE}=upk^*$,否则,运行 K^{PKE} 来产生 (upk_i^{PKE},upk^*),并且将 $(ID_i,partial\_key_i,upk_i^{PKE},usk_i^{PKE})$ 存储在数据库中,返回 upk_i^{PKE}。

RevealSecretKey:输入 ID_i,如果 $i=l$,终止运行,否则在数据库中查询 ID_i 用户私密密钥 usk_i^{PKE},如果存在则返回给 $\mathscr{B}_{Ⅱ}$,否则返回 $\perp$。

ReplaceKey:输入 ID_i 和 (upk^*,usk^*),如果 $i=l$,$\mathscr{C}_{Ⅱ}$ 终止运行,否则如果 ID_i 已经被创建,则 $\mathscr{C}_{Ⅱ}$ 使用 upk^* 替换 ID_i 的公钥,使用 usk^* 替换 ID_i 的私钥。否则不执行任何操作。

在攻击阶段,$\mathscr{B}_{Ⅱ}$ 输出两个消息 (m_0,m_1) 和一个目标身份 ID^*。如果 $ID^* \neq ID_l$,则 $\mathscr{C}_{Ⅱ}$ 终止运行。否则将 (m_0,m_1) 作为攻击查询发送给 S^{PKE},其收到的回复消息为 $c^*=\varepsilon^{PKE}(pk^*,m_b)$,其中 b 为随机数,$b \in_R \{0,1\}$。该密文将被进一步加密为 $c^*=\varepsilon^{IBE}(mpk,ID^*,c^*)$,并作为对 $\mathscr{B}_{Ⅱ}$ 的攻击。

将 $\mathscr{C}_{Ⅱ}$ 对 S^{PKE} 中隐藏的比特 b 的推测输出作为 $\mathscr{B}_{Ⅱ}$ 的输出 $b' \in \{0,1\}$。如果 $\mathscr{B}_{Ⅱ}$ 成功,则 $\mathscr{C}_{Ⅱ}$ 同样取得成功。后者对于 $\mathscr{B}_{Ⅱ}$ 攻击的身份的推测成功率至少为 $1/q_{ID}$。

设 $c=CL\text{-}Encrypt^{CPA}(mpk,ID,upk_{ID},m;coin)$ 为上文 CL-ENC 的加密算法,其中 $coin$ 为 c 随机产生的。将上文描述的解密算法表示为 $CL\text{-}Decrypt^{CPA}(usk_{ID},partial\_key_{ID},c)$。将这种 CPA 安全的 CL-ENC 方案转换成一个 CCA 安全方案,Libert 和 Quisquater 给出了如下的改变,其中 *CL-Encrypt* 和 *CL-Decrypt* 的上标用 CCA 替换:

$$CL\text{-}Encrypt^{CCA}(mpk,ID,upk_{ID},m) := CL\text{-}Encrypt^{CPA}(mpk,ID,upk_{ID},m \parallel coin;r)$$

其中,$r=H(m \parallel coin \parallel upk_{ID} \parallel ID)$,$H$ 是一个 Hash 函数。为了安全分析,它被认为表现为一个随机预言。解密算法改动如下:

(1) 计算 $(m' \parallel coin') \leftarrow CL\text{-}Decrypt^{CPA}(usk_{ID},partial\_key_{ID},c)$。

(2) 如果输出为 $\perp$,则将 $\perp$ 作为最后输出并终止。否则,计算 $c' \leftarrow CL\text{-}Encrypt^{CPA}(mpk,ID,upk_{ID},m' \parallel coin';\Omega)$,其中 $\Omega=H(m' \parallel coin' \parallel upk_{ID} \parallel ID)$。

(3) 如果 $c'=c$,输出 m',否则输出 $\perp$。

推论 在第 2 部分定义的 Type Ⅰ和 Type Ⅱ中在随机预言模型条件下,上

述改动是安全的。

通过在 Riyami 论文中定理 1 的证明来模拟附加的随机预言 H 和解密预言 $Decrypt$，可知 $\mathcal{B}_{\mathrm{I}}$ 和 $\mathcal{B}_{\mathrm{II}}$ 分别取得了 Type Ⅰ和 Type Ⅱ的成功。

6.7 Hwang 的模型

在 Libert 和 Quisquater 之后，Hwang 等人构建了一个 CCA 安全的 CL-PKE 方案，能抵抗 Type Ⅰ和 Type Ⅱ敌手。他们的方案是使用 Dent 在 2008 年提出的方式构建的，并采用 Boyen 在 2008 年提出的对 Waters 的 IBE 进行 2 级分层扩展来达到 CCA 安全性的技术。为了应付恶意 KGC 攻击，他们的方案应用不同的公钥产生算法：

$Setup(1^k)$：KGC 选择 p 阶素数群 G 和 G_T 使得能构建一个对 $e: G \times G \rightarrow G_T$，选取 G 的一个生成元 g。它在 Z_p^* 中选取随机值 $\alpha, \beta, \mu', \mu_1, \cdots, \mu_n, \nu', \nu_1, \cdots, \nu_n$，并计算 $g_1 = g^{\alpha}, h = e(g^{\alpha}, g^{\beta}), u' = g^{\mu'}, u_1 = g^{\mu_1}, \cdots, u_n = g^{\mu_n}, v' = g^{\nu'}, v = g^{\nu_1}, \cdots, v_n = g^{\nu_n}$，其中 n 是二进制字符串表示的身份的长度。$H: \{0,1\}^* \rightarrow \{0,1\}^n$ 是抗冲突的哈希函数。主公钥 mpk 和主私密密钥 msk 分别是：$mpk \leftarrow (e, G, G_T, g, g_1, h, u', u_1, \cdots, u_n, v', v_1, \cdots, v_n, H)$ 和 $msk \leftarrow (\alpha, \beta, \mu', \mu_1, \cdots, \mu_n, \nu', \nu_1, \cdots, \nu_n)$。

$PSK(mpk, msk, ID)$：ID 是一个长度为 n 的比特位串，$ID[i]$ 是第 i 个比特位。定义 $U \subset \{1, \cdots, n\}$ 是使得 $ID[i] = 1$ 的索引 i 的集合。KGC 挑选一个随机值 $r \in Z_p^*$ 并计算：

$$psk_{ID} = (psk_1, psk_2) = (g_1^{\beta} \cdot F_u(ID)^r, g^r)$$

其中，$F_u(ID) = u' \prod_{i \in U} u_i$，以 ID 为身份的用户被给定一个 psk_{ID} 作为部分私钥。

$UKeyGen(mpk, psk_{ID})$：选择一个私密值 $x_{ID} \in Z_p$。公钥 pk_{ID} 这样产生 $pk_{ID} = (X_{ID}, \sigma_{ID})$，其中 $X_{ID} = h^{x_{ID}}$，σ_{ID} 是 Schnorr 一次性签名，它使用 x_{ID} 作为签名密钥，以 $(h, X_{ID} = h^{x_{ID}})$ 作为认证密钥。消息可以是任意的字符串，只要它能够被包含在 mpk 中。签名是使用 Bellare 在 2007 年提出的没有随机预言的 Fiat-Shamir 转换技术产生的。然后它从 Z_p^* 随机地挑选 r' 并计算私钥 sk_{ID}：

$$(sk_1, sk_2) = (psk_1^{x_{ID}} \cdot F_u(ID)^{r'}, psk_2^{x_{ID}} \cdot g^{r'}) = (g_1^{\beta x_{ID}} \cdot F_u(ID)^{r x_{ID} + r'}, g^{r x_{ID} + r'})$$

$Enc(mpk, ID, pk_{ID}, m)$：对消息 $m \in G_T$ 进行加密，首先验证公钥 X_{ID} 是否被正确地形成，使用 (h, X_{ID}) 作为认证密钥，验证 σ_{ID} 是否为一个有效的签名。如果为能满足，输出 $\perp$ 并终止算法。否则，选择一个随机值 $s \in Z_p^*$ 并计算（w 是一个 n 位比特串，w_i 是 w 的第 i 个比特位）：

$$c = (C_0, C_1, C_2, C_3) = (m \cdot (X_{ID})^s, g^s, F_u(ID)^s, F_v(w)^s)$$

其中，$w = H(C_0, C_1, C_2, ID, pk_{ID}) \in \{0,1\}^n$，$F_v(w) = v' \prod_{j=1}^{n} v_j^{w_j}$。

$Dec(mpk, sk_{ID}, c)$：对密文 $c = (C_0, C_1, C_2, C_3)$，验证

$$e(C_1, F_u(ID) \cdot F_v(w)) = e(g, C_2 C_3)$$

其中 $w = H(C_0, C_1, C_2, ID, pk_{ID}) \in \{0,1\}^n$。如果不满足，输出 $\perp$，否则计算 $m = C_0 \cdot e(C_2, sk_2)/e(C_1, sk_1)$。

安全性证明：Hwang 等人证明了上面的构建在标准模型中决定性双线性 Diffie-Hellman（DBDH）假定下对恶意 KGC 是安全的。

定理 6.3　$\mathcal{A}_{\text{II}}$ 是 Type Ⅱ 敌手，它至多产生 q_d 次解密询问和 q_{pk} 次公钥询问，那么得到 $Adv^{CL}_{\mathcal{A}_{\text{II}}} \leqslant 4q_{pk}q_d(n+1) \cdot Adv^{DBDH}_{\mathcal{A}'}(k) + q_{pk} \cdot Adv^{CR}_{\mathcal{A}''}(k)$。其中，$\mathcal{A}'$ 和 $\mathcal{A}''$ 是与 $\mathcal{A}_{\text{II}}$ 同时运行的算法。

证明：Hwang 等人定义一系列的修改后的攻击游戏。每个游戏都是在相同的可能性空间中操作的。攻击者尝试区分隐藏的比特位 b 和最终输出的猜测的比特位 b'，其中隐藏比特位 b 在整个游戏中都是使用同一个值，而有些规则定义了一个模拟者对预言询问的回应因游戏不同而有差异。

S_i 是在游戏 i 中事件 $b' = b$，Adv_i 表示在游戏 i 中的敌手优势。那么 $Adv_i = |Pr[S_i] - 1/2|$。从游戏 1 开始，并说明 $i > 1$ 的游戏 i 的定义，其中当且仅当 $Adv_i = |Pr[S_{i-1}] - 1/2|$ 是可忽略的，$Adv_i = |Pr[S_i] - 1/2|$ 才是可忽略的。事件 E 表示在执行敌手期间发生的，而且它是和 S_i 相互独立的（例如 $Pr[S_i \mid E] = Pr[S_i]$）。游戏 $i+1$ 是一个攻击环境，除了事件 E 发生时，它和游戏 i 是等同的。如果事件 E 没有发生，敌手就会在游戏 $i+1$ 中选择与游戏 i 使用的相同的比特位（比如，$Pr[S_{i+1} \mid \neg E] = Pr[S_i \mid \neg E] = Pr[S_i]$）；否则，就会输出一个随机比特位 b'（比如 $Pr[S_{i+1} \mid E] - 1/2$）。那么得出：

$$\begin{aligned} |Pr[S_{i+1}] - 1/2| &= |Pr[S_{i+1} \mid E]Pr[E] + Pr[S_{i+1} \mid \neg E]Pr[\neg E] - 1/2| \\ &= |Pr[E]/2 + Pr[S_i \mid \neg E]Pr[\neg E] - 1/2| \\ &= |(1 - Pr[\neg E])/2 + Pr[S_i]Pr[\neg E] - 1/2| \\ &= Pr[\neg E]\,|Pr[S_i] - 1/2| \end{aligned}$$

因此有 $Adv_{i+1} = Pr[\neg E] \cdot Adv_i$。

Game 1：这个游戏和原来的攻击环境一样。Type Ⅱ 敌手 $\mathcal{A}_{\text{II}}$ 首先输出 (mpk, msk) 给模拟者 $\mathcal{B}$，并和 $\mathcal{B}$ 进行交互。$\mathcal{A}_{\text{II}}$ 分别向 *PKO*，*SKO* 和 *DecO* 提交至多 q_{pk}，q_{sk} 和 q_d 次询问。定义下面的集合：

$pk_L = \{ID_1, \cdots, ID_{q_{pk}}\}$：询问公钥预言的身份集合。

$sk_L = \{ID'_1, \cdots, ID'_{q_{sk}}\}$：询问私钥提取预言的身份集合。

$D_w = \{w_1, \cdots, w_{q_d}\}$：包含在解密询问中的字符串 $w_j = H(C_0, C_1, C_2, ID_j, pk_j)$

的集合。

$\mathcal{A}_{\mathrm{II}}$ 选择一个目标身份/公钥对 (ID^*, pk_{ID^*}) 和两个等长的消息 m_0, m_1，其中 $ID^* \notin sk_L$，然后将他们发送给 $\mathcal{B}$。它被指定 $c^* = (C_0^*, C_1^*, C_2^*, C_3^*)$ 作为挑战密文。设 $w^* = (C_0^*, C_1^*, C_2^*, ID^*, pk_{ID^*})$ 和 $w^* \notin D_w$。

Game 2：在这个游戏中，$\mathcal{B}$ 首先在 pk_L 中随机选择一个身份 ID_i。g^a, g^b 是随机元素使得 a, b 对 $\mathcal{B}$ 都是未知的。然后使用 $e(g^a, g^b)^{\alpha\beta}$ 设置 X_{ID_i}。此时，x_{ID_i} 被认为是 ab，因为 $h = e(g^\alpha, g^\beta)$. π_{ID_i} 能够像在一次性签名中的签名预言那样被模拟。它挑选一个 $\kappa \in \{0, \cdots, n\}$，$\tau$ 是一个整数使得 $\tau(n+1) < p$。而且，它从 Z_τ 中随机地选择向量 $(x', x_1, \cdots, x_n)$，从 Z_p 选择 $(y', y_1, \cdots, y_n)$ 并设置：

$$v' = (g^a)^{x' - \kappa\tau}, v_j = (g^a)^{x_j} g^{y_j} (1 \leqslant j \leqslant n)$$

如果 $\mathcal{A}$ 没有选择 ID_i 作为目标身份（即 $ID_i \neq ID^*$），那么 $\mathcal{B}$ 终止。因此，$Adv_2 = \frac{1}{q_{pk}} Adv_1$。

Game 3：游戏 3 和游戏 2 等同，除了下面的情况：对于已经形成的密文 $c = (C_0, C_1, C_2, C_3)$，其中 w 或者与之前提交的密文有相同的值，或者 w 和已经过去的挑战阶段的 w^* 相等，如果攻击者提交一个解密询问 (c, ID, pk_{ID})，那么 $\mathcal{B}$ 就终止。对于一个合法解密询问，有 $c \neq c^*$ 或者 $(ID, pk_{ID}) \neq (ID^*, pk_{ID^*})$。在任一例子中，这都暗示着 H 的冲突。因此，Hwang 等人构建算法 $\mathcal{A}''$，使得 $|Pr[S_2] - Pr[S_3]| \leqslant Adv^{CR}_{\mathcal{A}''}(k)$。

Game 4：根据 *Game* 2 中的值定义下面的函数：

$$J(w) = x' + \sum_{j=1}^{n} w_j x_j - \kappa\tau$$

$$K(w) = y' + \sum_{j=1}^{n} w_j x_j$$

输入 n 比特位字符串 $w = w_1 \cdots w_n$，然后计算 $F_v(w) = v' \prod_{j=1}^{n} v_j^{w_j} = (g^a)^{J(w)} \cdot g^{K(w)}$。

Game 4 和 *Game* 3 等同，除了下面的这种情况：在 $\mathcal{A}$ 输出它对 b 的猜测值 b' 后，$\mathcal{B}$ 验证是否 $J(w^*) = 0 (\mathrm{mod}\, p)$。如果 $J(w^*) \neq 0 (\mathrm{mod}\, p)$，那么 $\mathcal{B}$ 终止并且输出一个随机比特位 b'。事件 $J(w^*) = 0 (\mathrm{mod}\, p)$ 的发生是偶然的，因为 $\mathcal{A}_{\mathrm{II}}$ 并不知道计算 $J(w)$ 时关于值 $(x', x_1, \cdots, x_n, \kappa, \tau)$ 的任何信息。实际上，$Pr[J(w^*) = 0 (\mathrm{mod}\, p)] = Pr[\kappa\tau = (x' + \sum_{j=1}^{n} w_j x_j)]$，因为 $(x' + \sum_{j=1}^{n} w_j x_j) < \tau(n+1)$，$\kappa\tau < \tau(n+1)$ 和 $\tau(n+1) < p$。因此，$Pr[J(w^*) = 0 (\mathrm{mod}\, p)] = \frac{1}{\tau(n+1)}$，而且 $Adv_4 = \frac{1}{\tau(n+1)} Adv_3$。

Game 5：修改挑战密文的构建方法。$\mathcal{B}$ 引入一个新的变量 $\sigma \leftarrow Z_p^*$ 和 $C_1^* =$

g^{σ}。它翻转硬币 b,计算 $C_0^* = m_b \cdot X_{ID^*}^{\sigma}$, $C_2^* = C_1^{*U_{ID^*}} = (g^{\sigma})^{U_{ID^*}}$, $C_3^* = C_1^{*K(w^*)}$,其中 $w^* = H(C_0^*, C_1^*, C_2^*, ID^*, pk_{ID^*})$ 和 $U_{ID^*} = \sum_{i \in u} \mu_j$。很明显,$Adv_5 = Adv_4$。

Game 6:改变 *Game* 5,使得在 $\mathcal{A}$ 输出猜测值 b' 后,$\mathcal{B}$ 终止。对于一些 $w_{\ell} \in D_w$,其中 $\ell \in \{1, \cdots, q_d\}$,如果 $J(w_{\ell}) = 0 (\bmod \tau)$,使用一个随机比特位 b' 来替换 $\mathcal{A}$ 的输出。因为 $Pr[J(w) = 0 (\bmod \tau)] = 1/\tau$, $Adv_6 = \left(1 - \frac{1}{\tau}\right)^{q_d} \cdot Adv_5 \geqslant \left(1 - \frac{q_d}{\tau}\right) \cdot Adv_5$ 就同 $Pr[J(w) = 0 (\bmod \tau)] = 1/\tau$。如果设 $\tau = 2q_d$,那么 $Adv_6 \geqslant \frac{1}{2} Adv_5$。

Game 7:Hwang 等人有效地改变对 $\mathcal{A}$ 的询问的处理。对于所有不包括 ID^* 公钥询问、私钥询问和解密询问,$\mathcal{B}$ 能够通过运行算法 $PSK(mpk, msk, ID)$、$UKeyGen(mpk, psk_{ID})$ 和 $Dec(mpk, sk_{ID}, c)$ 来响应询问。而且,它对所有包含 ID^* 的解密询问进行如下的响应:当它收到关于 ID^* 的有效密文 (C_0, C_1, C_2, C_3) 的解密询问,$\mathcal{B}$ 终止,并如 Game 6 中那样,如果 $J(w) = 0 (\bmod \tau)$,就输出一个随机比特位 b'。否则,$\mathcal{B}$ 通过如下计算来提取消息 m:

$$w \leftarrow H(C_0, C_1, C_2, ID^*, pk_{ID^*})$$

$$(g^a)^s \leftarrow (C_3 / C_2^{K(w)})^{1/J(w)}$$

$$m \leftarrow C_0 / e(g^{as}, g^b)^{\alpha\beta} = C_0 / e(g^{\alpha}, g^{\beta})^{abs} = C_0 / X_{ID^*}^s.$$

注意,可以计算 $(C_3 / C_1^{K(w)})^{1/J(w)}$,因为如果 $J(w) = 0 (\bmod \tau)$ 则 $J(w) \neq 0 (\bmod p)$。并且和在 *Game* 6 中一样,$\mathcal{B}$ 能正确地回答 $\mathcal{A}$ 的询问。这就是暗示了 $Adv_7 = Adv_6$。

Game 8:再次更改挑战密文的产生。对于 *Game* 5 中引入的变量 σ,使得 $C_1^* = g^{\sigma}$ 和 $Z = e(g^a, g^b)^{\sigma}$。$\mathcal{B}$ 检索 α, β 的值,翻转硬币 b,并计算 $C_0^* = m_b \cdot Z^{\alpha\beta}$, $C_2^* = (g^{\sigma})^{U_{ID^*}}$, $C_3^* = c(g^{\sigma})^{K(w^*)}$,其中 $w^* = H(C_0^*, C_1^*, C_2^*, ID^*, pk_{ID^*})$。有 $Adv_8 = Adv_7$。

Game 9:改变挑战阶段。这次 $\mathcal{B}$"忘记"σ 的值,只是简单地保留 C_1^*。挑战密文的构建和 Game 8 中相同,但是这次使用一个随机选取的 $Z \in G_T$。整个模拟只依赖于值 g^a, g^b, g^{σ} 并且模拟者根本就不使用 a, b, σ。因此,$|Pr[S_8] - Pr[S_9]| \leqslant Adv_{\mathcal{A}'}^{DBDH}(k)$,而且 $Pr[S_9] = 1/2$,有:

$$Adv_6 = Adv_7 = Adv_8 \leqslant Adv_{\mathcal{A}'}^{DBDH}(k)$$

$$Adv_4 = Adv_5 \leqslant 2 \cdot Adv_6$$

因为 $Adv_4 = Adv_3 / (\tau(n+1))$ 并且 $\tau = 2q_d$,得出:

$$Adv_3 \leqslant 4q_d(n+1) \cdot Adv_{\mathcal{A}'}^{DBDH}(k)$$

$$Adv_2 \leqslant Adv^{CR}_{\mathscr{B}''}(k) + Adv_3 \leqslant 4q_d(n+1) \cdot Adv^{DBDH}_{\mathscr{B}'}(k) + Adv^{CR}_{\mathscr{B}''}(k)$$

最后，因为 $Adv_2 = \frac{1}{q_{pk}} Adv_1$，得出：

$$Adv_1 \leqslant 4q_{pk}q_d(n+1) \cdot Adv^{DBDH}_{\mathscr{B}'}(k) + q_{pk} \cdot Adv^{CR}_{\mathscr{B}''}(k)$$

针对 Type Ⅰ敌手的安全证明：

定理 6.4 $\mathscr{A}_{\mathrm{I}}$ 是 Type Ⅰ敌手，它至多产生 q_d 次解密询问，那么有

$$Adv^{CL}_{\mathscr{A}_{\mathrm{I}}} \leqslant 4q_d(n+1) \cdot Adv^{DBDH}_{\mathscr{B}'}(k) + Adv^{CR}_{\mathscr{B}''}(k) + Adv^{OT}_{\mathscr{A}_s}(k)$$

其中，$\mathscr{A}'$，$\mathscr{A}''$和 $\mathscr{A}_s$ 是同时运行的算法。

证明：它和定理 6.3 的证明方式类似。

Game 1：这个游戏和原来的攻击环境一样。$\mathscr{B}$ 运行 $Setup(1^k)$，输出（mpk，msk）。Type Ⅰ敌手 $\mathscr{A}_{\mathrm{I}}$ 被指定了 mpk，然后 $\mathscr{A}_{\mathrm{I}}$ 分别向 $PSKO$，PKO，$RepO$，SKO 和 $DecO$ 提交至多 q_{psk}，q_{pk}，q_{rpk}，q_{sk}和 q_d 次询问。定义下面的集合：

$pk_L = \{ID_1, \cdots, ID_{q_{pk}}\}$：询问公钥预言的身份集合；

$rpk_L = \{ID_1, \cdots, ID_{q_{rpk}}\}$：询问私钥替换预言的身份集合；

$psk_L = \{ID'_1, \cdots, ID'_{q_{psk}}\}$：询问部分私钥提取预言的身份集合；

$D_w = \{w_1, \cdots, w_{q_d}\}$：包含在解密询问中的字符串 $w_j = H(C_0, C_1, C_2, ID_j, pk_j)$ 的集合；

$\mathscr{A}_{\mathrm{I}}$ 选择一个目标身份/公钥对（ID^*，pk_{ID^*}）和两个等长的消息 m_0, m_1，其中 $ID^* \notin psk_L$ 或者 $ID^* \notin rpk_L$，然后将他们发送给 $\mathscr{B}$。他被指定 $c^* = (C_0^*, C_1^*, C_2^*, C_3^*)$作为挑战密文。设 $w^* = (C_0^*, C_1^*, C_2^*, ID^*, pk_{ID^*})$和 $w^* \notin D_w$。

Game 2：这个游戏和 *Game* 1 一样，除了系统参数 mpk 的一些是以下面的方式来替换：在 G 中 g^a 是随机元素使得 a 对 $\mathscr{B}$ 是未知的。它随机地选择 $\beta \in Z_p^*$，并设置 $g_1 = g^a$，$h = (g^a, g^\beta)$。而且它挑选一个 $\kappa_v \in \{0, \cdots, n\}$，$\tau$ 是一个整数使得 $\tau(n+1) < p$。而且，它从 Z_{τ_v} 中随机地选择向量 $(x'_v, x_{v,1}, \cdots, x_{v,n})$，从 Z_p 选择 $(y'_v, y_{v,1}, \cdots, y_{v,n})$并设置：$v' = (g^a)^{x'_v - \kappa_v \tau_v} g^{y'_v}$，$v_j = (g^a)^{x_{v,j}} g^{y_{v,j}} (1 \leqslant j \leqslant n)$。

替换后的公钥和之前的游戏中产生的公钥具有相同的分布。它也包含一个有效的一次性签名 π。因此，能够构建一个算法 $\mathscr{A}_s$ 使得 $|Pr[S_1] - Pr[S_2]| \leqslant Adv^{OT}_{\mathscr{A}_s}(k)$。注意 $(v_1, \cdots, v_n)$和 msk 的 α（被认为是 a）对 $\mathscr{B}$ 是不可知的。不过，它仍然能够保证 msk 其他值 $(\beta, \mu', \mu_1, \cdots, \mu_n, v')$是安全的。

Game 3：在这个游戏中，$\mathscr{B}$ 首先在 pk_L 中随机选择一个身份 ID_i。在 G 中 g^b 是随机元素使得 b 对 $\mathscr{B}$ 是未知的。然后使用 $e(g^a, g^{b\beta})$设置 X_{ID_i}。此时，x_{ID_i}被认为是 b，因为 $h = e(g^a, g^\beta)$。可以看到 $Adv_3 = Adv_2$。

Game 4：这个和 *Game* 3 等同，除了下面的情况：对于已经形成的密文 $c = (C_0, C_1, C_2, C_3)$，其中 w 或者与之前提交的密文有相同的值，或者 w 和已经过去

的挑战阶段的 w^* 相等，如果攻击者提交一个解密询问 (c, ID, pk_{ID})，那么 $\mathcal{B}$ 就终止。对于一个合法解密询问，有 $c \neq c^*$ 或者 $(ID, pk_{ID}) \neq (ID^*, pk_{ID^*})$。在任一例子中，这都暗示着 H 的冲突。因此，构建一个算法 $\mathcal{A}''$，使得 $|Pr[S_3] - Pr[S_4]| \leqslant Adv^{CR}_{\mathcal{A}''}(k)$。

Game 5：根据 *Game* 3 中的值定义下面的函数：

$$J(w) = x' + \sum_{j=1}^{n} w_j x_j - \kappa\tau$$

$$K(w) = y' + \sum_{j=1}^{n} w_j x_j$$

输入 n 比特位字符串 $w = w_1 \cdots w_n$，然后 $F_v(w) = v' \prod_{j=1}^{n} v_j^{w_j} = (g^a)^{J(w)} \cdot g^{K(w)}$。

Game 5 和 *Game* 4 等同，除了下面的这种情况：在 $\mathcal{A}$ 输出它对 b 的猜测值 b' 后，$\mathcal{B}$ 验证是否 $J(w^*) = 0 (\mathrm{mod}\, p)$。如果 $J(w^*) \neq 0 (\mathrm{mod}\, p)$，那么 $\mathcal{B}$ 终止并且输出一个随机比特位 b'。事件 $J(w^*) = 0 (\mathrm{mod}\, p)$ 的发生是偶然的，因为 $\mathcal{A}_{\mathrm{II}}$ 并不知道计算 $J(w)$ 时关于值 $(x', x_1, \cdots, x_n, \kappa, \tau)$ 的任何信息。实际上，$Pr[J(w^*) = 0 (\mathrm{mod} p)] = Pr[\kappa\tau = (x' + \sum_{j=1}^{n} w_j x_j)]$，因为 $(x' + \sum_{j=1}^{n} w_j x_j) < \tau(n+1)$，$\kappa\tau < \tau(n+1)$ 和 $\tau(n+1) < p$。因此，$Pr[J(w^*) = 0 (\mathrm{mod}\, p)] = \dfrac{1}{\tau(n+1)}$，而且 $Adv_5 = \dfrac{1}{\tau(n+1)} Adv_4$。

Game 6：修改挑战密文的构建方法。$\mathcal{B}$ 引入一个新的变量 $\sigma \leftarrow Z_p^*$ 和 $C_1^* = g^\sigma$。它翻转硬币 b，计算 $C_0^* = m_b \cdot X_{ID^*}^c$，$C_2^* = C_1^{* U_{ID^*}} = (g^\sigma)^{U_{ID^*}}$，$C_3^* = C_1^{* K(w^*)} = (g^\sigma)^{K(w^*)}$，其中 $w^* = H(C_0^*, C_1^*, C_2^*, ID^*, pk_{ID^*})$ 和 $U_{ID^*} = \sum_{i \in u} \mu_j$。很明显，$Adv_6 = Adv_5$。

Game 7：改变 *Game* 6，使得在 $\mathcal{A}$ 输出猜测值 b' 后，$\mathcal{B}$ 终止。对于一些 $w_\ell \in D_w$，其中 $\ell \in \{1, \cdots, q_d\}$，如果 $J(w_\ell) \equiv 0 (\mathrm{mod}\, \tau)$，使用一个随机比特位 b' 来替换 $\mathcal{A}$ 的输出。因为 $Pr[J(w) \equiv 0 (\mathrm{mod}\, \tau)] = 1/\tau$，$Adv_6 = \left(1 - \dfrac{1}{\tau}\right)^{q_d} \cdot Adv_5 \geqslant \left(1 - \dfrac{q_d}{\tau}\right) \cdot Adv_5$。设 $\tau = 2q_d$，那么 $Adv_7 \geqslant \dfrac{1}{2} Adv_6$。

Game 8：有效地改变对 $\mathcal{A}$ 的询问的处理。对于所有不包括 ID^* 公钥询问，私钥询问和解密询问，$\mathcal{B}$ 能够通过运行算法 $PSK(mpk, \beta, ID)$（对于被询问的 ID 要产生 psk_{ID} 只要求 msk 中的 β，而不是 msk），$UKeyGen(mpk, psk_{ID})$ 和 $Dec(mpk, sk_{ID}, c)$ 来响应询问。当它收到一个公钥替换询问时，它使用新的公钥 pk'_{ID} 来替换之前产生的身份 ID 的公钥 pk_{ID}。如果解密询问包含了身份 ID 的替换后的公钥，那么相应的私钥 x_{ID} 也要求提供。否则就终止。而且，它对所有包含 ID^* 的

解密询问进行如下的响应：当它收到关于 ID^* 的有效密文 (C_0, C_1, C_2, C_3) 的解密询问，$\mathcal{B}$ 终止并如 *Game* 6 中那样，如果 $J(w) \equiv 0 \pmod{\tau}$，就输出一个随机比特位 b'。否则，$\mathcal{B}$ 通过如下计算来提取消息 m：

$$w \leftarrow H(C_0, C_1, C_2, ID^*, pk_{ID^*})$$

$$(g^a)^s \leftarrow (C_3 / C_2^{K(w)})^{1/J(w)}$$

$$m \leftarrow C_0 / e(g^{as}, B)^{\beta} = C_0 / e(g^{\alpha}, g^{\beta})^s = C_0 / X_{ID}^s.$$

其中，如果 $ID^* \notin rpk_L$，那么 $B = g^b$，否则 $B = g^{x_{ID^*}}$，因为如果 $ID^* \in rpk_L$，x_{ID}。就应该被指定解密预言。注意，可以计算 $(C_3 / C_1^{K(w)})^{1/J(w)}$，因为如果 $J(w) \equiv 0 \pmod{\tau}$ 则 $J(w) \neq 0 \pmod{p}$。还注意到能像在 *Game* 6 中一样，$\mathcal{B}$ 能正确地回答 $\mathcal{A}$ 的询问。这就是暗示了 $Adv_8 = Adv_7$。

Game 9：再次更改挑战密文的产生。对于 *Game* 6 中引入的变量 σ，使得 $C_1^* = g^{\sigma}$ 和 $Z = e(g^a, g^b)^{\sigma}$。$\mathcal{B}$ 检索 α, β 的值，翻转硬币 b，并计算 $C_0^* = m_b \cdot Z^{\beta}$，$C_2^* = (g^{\sigma})^{U_{ID^*}}$，$C_3^* = C(g^{\sigma})^{K(w^*)}$，其中 $w^* = H(C_0^*, C_1^*, C_2^*, ID^*, pk_{ID^*})$。有 $Adv_9 = Adv_8$。

Game 10：改变挑战阶段。这次 $\mathcal{B}$ "忘记" σ 的值，只是简单地保留 C_1^*。挑战密文的构建和 Game 9 中相同，但是这次使用一个随机选取的 $Z \in G_T$。整个模拟只依赖于值 g^a, g^b, g^{σ} 并且模拟者根本就不使用 a, b, σ。因此，$|Pr[S_9] - Pr[S_{10}]| \leq Adv_{\mathcal{A}'}^{DBDH}(k)$，而且 $Pr[S_{10}] = 1/2$，所以有：

$$Adv_7 = Adv_8 = Adv_9 \leq Adv_{\mathcal{A}'}^{DBDH}(k)$$

$$Adv_5 = Adv_6 \leq 2 \cdot Adv_7$$

由 $Adv_5 = Adv_4 / (\tau(n+1))$ 并且 $\tau = 2q_d$，可得：

$$Adv_4 \leq 4q_d(n+1) \cdot Adv_{\mathcal{A}'}^{DBDH}(k)$$

$$Adv_3 \leq Adv_{\mathcal{A}''}^{CR}(k) + Adv_4 \leq 4q_d(n+1) \cdot Adv_{\mathcal{A}'}^{DBDH}(k) + Adv_{\mathcal{A}''}^{CR}(k)$$

最后，由 $Adv_3 = Adv_2$ 和 $Adv_1 \leq Adv_{\mathcal{A}_s}^{OT}(k) + Adv_2$，可得：

$$Adv_1 \leq 4q_d(n+1) \cdot Adv_{\mathcal{A}'}^{DBDH}(k) + Adv_{\mathcal{A}''}^{CR}(k) + Adv_{\mathcal{A}_s}^{OT}(k)$$

参考文献

[1] Galindo D, Morillo P, Rafols C. Breaking Yum and Lee generic constructions of certificateless and certificate-based encryption schemes, Lecture notes in computer science, 2006, Vol. 4043: 81-91.

[2] Al-Riyami S, Paterson K G. Certificateless public key cryptography, Lecture notes in computer science, 2003, Vol. 2894: 452-473.

[3] Al-Riyami S, Paterson K G. CBE from CL-PKE: A generic construction and efficient

scheme, Lecture notes in computer science,2005, Vol. 3386:398-415.

[4] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing, Lecture notes in computer science,2005, Vol. 3650:134-148.

[5] Bellare M, Desai A, Pointcheval D, Rogaway P. Relations among notions of security for public-key encryption schemes, Lecture notes in computer science,1998, Vol. 1462:26-45.

[6] Bentahar K, Farshim P, Malone-Lee J, Smart N P. Generic constructions of identity-based and certificateless kEMs, Journal of cryptology, 2005, Vol. 21, No. 2.

[7] Boneh D, Franklin M. Identity-based encryption from the weil pairing, Lecture notes in computer science,2001, Vol. 2139:213-229.

[8] Canetti R, Goldreich O, Halevi S. The random oracle methodology, Journal of the ACM, 2004, Vol. 51, No. 4:557-594.

[9] Dodis Y, Katz J. Chosen-ciphertext security of multiple encryption, Lecture notes in computer science,2005, Vol. 3378:188-209.

[10] Gentry C. Certificate-based encryption and the certificate-revocation problem, Lecture notes in computer science,2003, Vol. 2656:272-291.

[11] Hwang Y H, Liu J K, Chow S S M. Certificateless public key encryption secure against malicious KGC attacks in the standard model, Journal of universal computer science,2008, Vol. 14, No. 3:156-161.

[12] Bellare M. Two-tier signatures, strongly unforgeable signatures and Fiat-Shamir without random oracles, Lecture notes in computer science, 2007, Vol. 4450:201-216.

[13] Boyen X, Mei Q. Direct chosen ciphertext security from identity-based techniques, Proc. ACMCCS 2005,2009:320-329.

[14] Chow S, Boyd C. Security-mediated certicateless cryptography, Lecture notes in computer science,2006, Vol. 3958:508-524.

[15] Galindo D, Rfiafols P. Breaking Yum and Lee generic constructions of certificate-less and certificate-based encryption schemes, Lecture notes in computer science,2006, Vol. 4043: 81-91.

[16] Hu B, Zhang D W, Deng Z. Key replacement attack against a generic construction of certificateless signature, Lecture notes in computer science,2006, Vol. 4058:235-246.

[17] Libert B, Quisquater. On constructing certificateless cryptosystems from identity based encryption, Lecture notes in computer science,2006, Vol. 3958:474-490.

[18] Liu J, Au M, Susilo. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model, Proc. ASIACCS 2007,2007:273-283.

[19] Shamir A. Identity-based cryptosystems and signature schemes, Lecture notes in computer science,1984, Vol. 196:47-53.

[20] Waters B. Efficient identity-based encryption without random oracles, Lecture notes in computer science,2005, Vol. 3494:114-127.

[21] Yum D, Lee. Generic construction of certificateless encryption, Lecture notes in computer

science,2004, Vol. 3043:802-811.

[22] Yum D, Lee. Identity-based cryptography in public key management, Lecture notes in computer science,2004, Vol. 3093:71-84.

[23] Boneh D, Franklin M. Identity based encryption from the weil pairing, Lecture notes in computer science,2001, Vol. 2139:213-229.

[24] Rackoff C, Simon D. Non-interactive zero-knowledge proof of knowledge and chosen cipher text attack, Lecture notes in computer science,1991, Vol. 547:433-444.

[25] Huang Q, Wong D S. Generic certificateless encryption secure against malicious-but-passive KGC attacks in the standard model, Journal of computer science and Technology, 2007, Vol. 25, No. 4:807-826.

[26] Abe M, Cui Y, Imai H, Kiltz E. Efficient hybrid encryption from ID-based encryption, Journal of cryptology,2007, Vol. 21, No. 1:97-130.

[27] Au M H, Chen J, Liu J K, et al. Malicious KGC attacks in certificateless cryptography, In ACM ASIACCS'07,2007:302-311.

[28] Abe M, Gennaro R, Kurosawa K, Shoup V. A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM, Lecture notes in computer science,2005, Vol. 3494:128-146.

[29] Boneh D, Boyen X. Short signatures without random oracles, Lecture notes in computer science,2004, Vol. 3027:416-432.

[30] Boneh D, Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption, SIAM journal computing,2006, Vol. 36, No. 5:915-942.

[31] Boneh D, Katz J. Improved efficiency for cca-secure cryptosystems built using identity-based encryption, Lecture notes in computer science,2004, Vol. 3376:87-103.

[32] Chen L, Cheng Z, Malone-Lee J, Smart N. Efficient ID - KEM based on the Sakai-Kasahara key construction, IEEE proceedings-information security,2006, Vol. 153, No. 1: 19-26.

[33] Chalkias K, Hristu-Varsakelis D, Stephanides G. Improved anonymous timed-release encryption, Lecture notes in computer science,2007, Vol. 4734:311-326.

[34] Chow S M S, Roth V, Rieffel G E. General certificateless encryption and timed-release encryption, Lecture notes in computer science,2008, Vol. 5229:126-143.

[35] Cramer R, Shoup V. A practical public key cryptosystem provably secureagainst adaptive chosen ciphertext attack, Lecture notes in computer science,1998, Vol. 1462:13-25.

[36] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, SIAM journal computing,2003, Vol. 33,No. 1: 167-226.

[37] Dent A. A designer's guide to KEMs, In cryptography and codings, Lecture notes in computer science,2003, Vol. 2898:133-151.

[38] Even S, Goldreich O, Micali S. On-line/off-line digital signatures, Journal of cryptology,

1996, Vol. 9, No. 1:13.

[39] Gentry C. Practical identity-based encryption without random oracles, Lecture notes in computer science,2006, Vol. 4004:445-464.

[40] Huang X, Susilo W, Mu Y, Zhang F. On the security of certificateless signature schemes from Asiacrypt 2003, Lecture notes in computer science,2005, Vol. 3810:13-25.

[41] Menezes A, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field, IEEE transaction on information theory,1993, Vol. 39:1639-1646.

[42] Hu L, Nurbol, Lin L, Zhao K. An online unsupervised intrusion detection system based-on SVM. Proceedings of 2009 2nd IEEE international conference on broadband network & multimedia technology,2009:438-442.

[43] Hu L, Ren W, Ren F. Anomaly detection using improved hierarchy clustering. Proceedings of 2009 international conference on artificial intelligence and computational intelligence, 2009, Shanghai:319-323.

[44] Zhao K, Chu J, Che X, Lin L, Hu L. Improvement on rules matching algorithm of snort based on dynamic adjustment. Proceedings of the 2nd international conference on anti-counterfeiting, security and identification, Aug. 20-23,2008, Guiyang, China:285-287.

第七章　PKG 受约束的基于身份加密算法

7.1　PKG 受约束的基于身份加密算法介绍

由 Shamir 提出的基于身份加密的概念是一种简化公钥基础设施内的公钥和证书管理的方法。虽然这个概念在 1984 就被提出了，但是直到 2001 年才由 Boneh 和 Franklin 构建出第一个实用且功能完整的 IBE 方案。他们的方案使用了双线性映射的构建方式并且能够在随机预言机模型中被证明是安全的。随后，基于身份的密码学出现了飞速的发展，很多的文章提出了在更强的安全性概念下，如何构建高效的 IBE 方案。从而出现了分层的 IBE、基于身份的签名和认证方案，基于无证书的签名和加密方案等。

由于 PKG 有能力计算出任何身份所对应的私钥，那么它就需要彻底地被信任。也就是说这个 PKG 将可以随意地从事任何的恶意行为却不会面临任何法律制裁。这些恶意行为可能包括：解密和读取任意用户的信息，也可以为任何身份生成和分配私钥。尽管它具有很出色的性能，但事实上这已经成为减缓 IBE 使用的一个重要原因。由于存在密钥托管问题，IBE 的用户被限制在小的且封闭的组织中，该组织只有一个权威中心，这些都引起了对该形式的广泛争论。

目前有三种方案来解决该问题：一种是使用多 PKG 的方式。在这个方案中，IBE 系统的主密钥被分发给多个 PKG；即没有哪个单独的 PKG 有主密钥的完整信息。用门限方式为一个身份产生私钥。这是一个很有吸引力的解决方案，而且通过使用分布式的系统成功地避免了把全部信任都放在一个实体上的问题。但是这种解决方案是以采用额外的基础设施和通信设备为代价的。同时，这种方案需要用户向多个权威中心逐一证明自己的身份，并获取自己的私钥（通过一个安全通道完成），这对于用户来讲也是一种沉重的负担。况且在商业环境中，相对于管理一个单独的 PKG 来说，保持多个实体的独立是很困难的。另一种是无证书公钥密码方案（CL-PKE，certificateless public key encryption scheme）。该方案通过组合 IBE 方案和 PKI 体制的思想，使得用户的私钥由两个部分共同组成，且这两个部分分别独立地由 PKG 和用户生成，这样 PKG 并不知道整个私钥的内容。并且和 PKI 体制不同的是，CL-PKE 方案的 PKG 不再发布与用户所选取的部分私钥相对应的部分公钥的证书，而是直接发布该部分公钥，

即减少了证书生成过程。虽然 CL-PKE 方案从根本上解决了密钥托管问题,但是它却增加了对在线第三方的要求,来响应发送方对接收方部分公钥的询问。2007 年,Goyal 创造性地提出了第三种解决方案,该方案在不改变 IBE 方案的基础结构的条件下,减少了用户对 PKG 的信任需求,且该方案称为第三方权利受约束的 IBE 方案(A-IBE)。

在传统的 PKI 方案中,一个用户拥有一个由 CA 颁发并绑定了他的身份的公钥证书。如果 CA 再一次用该用户的身份产生一个公钥证书,则对应同一个身份的两个证书组成了一个用密码写成的 CA 欺诈的证据。在新方案中,PKG 是可以自由地为一个身份再一次产生解密密钥的,尽管两个对应于相同身份的解密密钥构成了一个欺诈的证据。当然他们之间截然不同,在传统的 PKI 中:CA 必须积极地将欺诈的证书发送给潜在的加密者(对 CA 来说是危险的)。而在 Goyal 的方案中,PKG 只是能够被动地解密用户信息。

2010 年,Xu 等人在 Goyal 提出的 A-IBE 方案的基础上进行了改进。通过尽可能地减少对运算的次数,提出了一个新的通用 A-IBE 方案,且新方案中对运算只在密文有效性验证阶段发生。更进一步地说,因为对运算是目前最有效的可以解决判定性 Diffie-Hellman(DDH)问题,而不破坏计算性 Diffie-Hellman(CDH)问题难解性的技术,该阶段的"对"运算具有必要性,即不可能再减少该处的"对"运算而不增加计算复杂性。Xu 方案在更强的安全性定义(在敌手完成私钥询问后,敌手可以适应性选择挑战 ID)下,基于一个更弱的难题(离散对数问题)实现了更有效的归约,新方案使得其安全性归约中仿真器的失败概率为 $1 = n$,其中 n 由用户选取,且当 n 等于敌手进行私钥询问的次数时该归约效率最优。

本章我们将分别介绍 Goyal 与 Xu 等人的第三方权利受约束的 IBE 方案,使读者全面了解这一方案的特点。

7.2 定义和模型

7.2.1 不经意传输

通俗来讲,一个 1/2 不经意传输协议允许接收方从发送方处精确地选择和接收 2 个串当中的 1 个。则接收者无法知道另外一个串,发送者也无法知道接收者到底选择了哪个串。这样就产生了各种各样基于特定(因式分解或 Diffie-Hellman)假设的 1/2 不经意传输的有效构建方式。

$1/n$ 不经意传输(OT_n^1)与 1/2 不经意传输(OT_2^1)类似,$1/n$ 不经意传输允许接收者从发送者所给的 n 个秘密中选取其中一个,且发送者无法知道接收者选择了哪一个,同时接收者也无法知道其他的秘密。OT_n^1 可以由 OT_2^1 通过通用的

方法构成,也可以通过密码技术直接构造。

7.2.2 基本模型

一个第三方权利受约束的基于身份的加密方案由如下 5 个算法组成:

初始化:这是一个随机的算法,该算法的输入是隐含参数。它输出是公开参数 PK 和一个主密钥 MK。

密钥产生:这是一个在公共参数生成器 PKG 和用户 U 之间的交互协议。给 PKG 和用户的共同输入为:公开参数 PK 和用户的身份 ID。给 PKG 的独有输入为主密钥 MK。另外,PKG 和 U 可能使用一个 0 或 1 的随机序列作为独有的输入。最后,U 获得一个解密密钥 d_{ID} 作为它的独有的输出。

加密:这是一个随机的算法,以下将作为输入:信息 m,身份 ID,和公开参数 PK。该算法的输出是密文 c。

解密:这个算法需要输入:在身份 ID 下被加密的密文 c,ID 的解密密钥 d_{ID} 和公开参数 PK。算法输出的是信息 m。

跟踪:这个算法将每个解密密钥都与一个解密密钥的族相关联。也就是说,这个算法将一个形式合法的解密密钥 d_{ID} 作为输入,并输出一个解密密钥组号 n_F。

在一个 A-IBE 系统中,有超级多项式个解密密钥族。每个身份 ID 的解密密钥 d_{ID} 都属于一个唯一的解密密钥族(用 n_F 表示)。简单地说,在安全性定义当中,需要已知属于一个族的解密密钥,它应该很难找到一个属于不同族的解密密钥(尽管它可能找到其他属于相同族的解密密钥)。

为了定义一个第三方权利受约束的基于身份的加密系统的安全性,首先定义以下的游戏。

IND-ID-CPA 游戏。A-IBE 的 IND-ID-CPA 游戏与标准 IBE 的 IND-ID-CPA 是十分相似的:

初始化:挑战者运行 A-IBE 的初始化算法并且将公共参数 PK 给敌手。

第一阶段:敌手和挑战者为一些不同的适应性选择身份 $ID^1,\cdots,ID^q$ 运行密钥产生协议并且获得解密密钥 $d_{ID^1},\cdots,d_{ID^q}$。

挑战:敌手提交两个等长的信息 m_0,m_1 并且身份 ID 不等于任何第一阶段中的身份询问的内容。挑战者随机在 0 和 1 中选择一个给 b,同时用 ID 加密 m_b。密文 c 将被传递给敌手。

第二阶段:除了敌手不被允许请求 ID 的解密密钥外,与第一阶段是相同。

猜测:敌手输出一个 b 的猜测 b'。

敌手在这个游戏中的优势定义为 $Pr[b'=b]-\frac{1}{2}$。

需要注意，由于考虑到阶段 1 和阶段 2 中的解密询问，以上的游戏将被扩展至可以处理选择密文攻击。可以称满足这种安全性的方案是 IND-ID-CCA 的。

FindKey 游戏。A-IBE 的 *FindKey* 游戏定义如下：

初始化：敌手（作为一个对抗性 PKG）产生并且将公开参数和身份 *ID* 传递给挑战者。挑战者对 *PK* 运行一个完整性检查并且如果检查失败的话将异常终止。

密钥产生：挑战者和敌手接下来根据密钥产生协议产生身份 *ID* 的解密密钥。挑战者和敌手接下来获取解密 d_{ID} 作为输出并且对它执行一个完整性检查，来确保它是形式合法的。如果检查失败将异常终止。

发现密钥：敌手输出一个解密密钥 d'_{ID}。挑战者对 d'_{ID} 执行一个完整性检查，如果检验失败将异常终止。

假设 *SF* 表示一个事件 $trace(d'_{ID}) = trace(d_{ID})$，即 d'_{ID} 和 d_{ID} 属于相同的解密密钥族。游戏中敌手的优势被定义为 $Pr[SF]$。

以上的游戏能够被扩展到包含解密阶段，在该阶段带有密文序列 $c_1, \cdots, c_m$ 的敌手适应的询问挑战者。挑战者用他的密钥 d_{ID} 解密 c_i 并且发送结果信息 m_i。如果敌手提交一个恶意结构的密文并且挑战者尝试去将它解密，则能够帮助敌手推断关于 d_{ID} 的解密密钥族的信息。

然而，如果敌手以某种方式被限制为只能够提交形式合法的密文，解密后的信息将保证不包含任何关于解密密钥族的信息（因为使用每个形式合法的密钥解密后的信息将相同）。这可以通过在解密过程中添加一个密文完整性检查获得。在这两种构建方式中，可以使用另外的方法给 *FindKey* 游戏添加一个解密步骤的方法。

ComputeNewKey 游戏。为 A-IBE 计算新密钥的游戏被定义如下：

初始化：挑战者执行 A-IBE 的初始化算法并且将公开参数 *PK* 给敌手。

密钥生成：敌手和挑战者为多个可区分的适应性选择身份 $ID^1, \cdots, ID^q$ 运行密钥生成协议，并且获得解密密钥 $d^1_{ID}, \cdots, d^q_{ID}$。

新密钥计算：敌手为身份 *ID* 输出 2 个解密密钥 d^1_{ID} 和 d^2_{ID}。挑战者在他们之间执行一个密钥完整性检验，如果检查失败，则异常终止。

设 *DF* 代表一个事件：$trace(d'_{ID}) \neq trace(d_{ID})$，即 d^1_{ID} 和 d^2_{ID} 属于不同的解密密钥族。在这个游戏中敌手的优势被定义为 $Pr[DF]$。可以定义一个选择 *ID* 计算新密钥的游戏，其中的敌手必须提前宣布身份 *ID*，它将为该 *ID* 做一个新的密钥计算。敌手的优势类似的被定义为是一个时间的概率，该事件可能从不同的解密密钥族中为每个宣布了身份的 *ID* 输出两个解密密钥。这个游戏的弱化与 IND-ID-CPA 游戏的弱化是相近的。

定义 7.1　如果所有多项式时间的敌手在 IND-ID-CPA 游戏、*FindKey* 游戏

和计算新密钥游戏中最多有一个可忽略的优势，则一个第三方权利受约束的基于身份的加密方案是 IND-ID-CPA 安全的。A-IBE 的 IND-ID-CCA 安全性的定义也与之相似。

7.3 Goyal 的 A-IBE 方案

7.3.1 基于 Gentry 方案的 A-IBE

Gentry 方案是现今已知的最有效的不需要随机预言机的 IBE 构建方式。除了较高的计算效率以外，它还拥有如较短的公开参数和较紧的安全性归约的性质。在不对基础密码系统做任何改变的情况下，就可以将 Gentry 的方案转变为 A-IBE 方案，能够按照基础的加密系统的需求构建一个安全密钥产生协议，并且在 A-IBE 模型的 3 个游戏中，安全性证明显示敌手的优势是可忽略的。证明基于 truncated q-ABDHE 和 q-SDH 假设，最终的结果是 A-IBE 方案与已知最好的无需随机语言机的 IBE 方案同样有效。

1. 构造方式

设 G_1 是一个阶为素数 p 的双线性群，且设 g 是 G_1 的生成元。另外，设 $e:G_1 \times G_1 \rightarrow G_2$ 表示一个双线性映射。安全性参数 κ 将决定群的大小。

如前所讨论的，基础的密码系统（即，初始化、加密和解密）与 Gentry 的密码系统是相同的。A-IBE 方案描述如下：

初始化 PKG 挑选随机生成元 $g, g_1, h_1, h_2, h_3 \in G_1$ 并且一个随机的 $\alpha \in Z_p$。它设定 $g_1 = g^{\alpha}$，公开的公共参数 PK 和主密钥 MK 由 $PK = g, g_1, h_1, h_2, h_3$ 和 $MK = \alpha$ 得出。

另外，假设一个函数 H 是一个普通的单向 Hash 函数。

密钥产生协议是带有身份 ID 的用户 U 能够通过该协议从 PKG 上安全地获取一个解密密钥 d_{ID}。如果 $ID = \alpha$，则 PKG 异常终止。密钥产生协议执行过程如下：

（1）用户 U 随机选择一个 $r \in Z_p$ 并且将 $R = h_1^r$ 发送给 PKG。

（2）U 将一个与 h_1 相关的 R 的离散对数以零知识证明的方式展示给 PKG。

（3）现在 PKG 选择 3 个随机数 $r', r_{ID,2}, r_{ID,3} \in Z_p$，然后计算 $(r', h'_{ID,1}), (r_{ID,2}, h_{ID,2}), (r_{ID,3}, h_{ID,3})$，其中 $h'_{ID,1} = (Rg^{-r'})^{1/(\alpha - ID)}$ 且 $h_{ID,i} = (h_i g^{-r_{ID,i}})^{1/(\alpha - ID)}$，$i \in \{2, 3\}$，并发送他们到用户 U。

（4）U 计算 $r_{ID,1} = r'/r$ 和 $h_{ID,1} = (h'_{ID,1})^{1/r}$，其中，$h'_{ID,1} = (h_1^r g^{-r'})^{1/(\alpha - ID)}$，$h_{ID,1} = ((h_1^r)^{1/r}(g^{-r'})^{1/r})^{1/(\alpha - ID)} = (h_1 g^{-r_{ID,1}})^{1/(\alpha - ID)}$。它计算解密密钥 $d_{ID} = \{(r_{ID,i}, h_{ID,i}) : i \in \{1,2,3\}\}$。

(5) U 现在对 d_{ID} 运行一个密钥完整性检验如下:它计算 $g^{\alpha-ID}=g_1/g^{ID}$ 并且检查 $e(h_{ID,i},g^{\alpha-ID})=e(h_i g^{-r_{ID,i}},g)$ 是否成立($i\in\{1,2,3\}$)。如果对于任意 i 检查失败则 U 异常终止。

最后,U 获得身份 ID 的一个形式合法的解密密钥 d_{ID}。

加密过程使用身份 $ID\in Z_p$ 加密一个信息 $m\in G_2$,产生一个随机的 $s\in Z_p$ 且计算密文 c 如下:

$$c=(g_1^s g^{-s\cdot D},e(g,g)^s,m\cdot e(g,h_1)^{-s},e(g,h_2)^s e(g,h_3)^{s\beta})$$

其中,由于 $c=(u,v,w,y)$,可设定 $\beta=H(u,v,w)$。

解密一个身份 ID 的密文 $c=(u,v,w,y)$,设定 $\beta=H(u,v,w)$ 并且测试 $y=e(u,h_{ID,2}h_{ID,3}^{\beta})^{v^{r_{ID,2}+r_{ID,3}\beta}}$ 是否成立,如果检查失败,就输出 $\perp$;否则就输出 $m=w\cdot e(u,h_{ID,1})v^{r_{ID,1}}$。

需要注意,在解密算法中的密文完整性检查拒绝所有无效的密文。

追踪:这个算法取得一个形式合法的解密密钥 $d_{ID}=\{(r_{ID,i},h_{ID,i}):i\in\{1,2,3\}\}$ 并输出解密密钥族号 $n_F=r_{ID,1}$。因此如果 $r_{ID,1}=r'_{ID,1}$,则对于两个解密密钥 d_{ID} 和 d'_{ID},$trace(d'_{ID})=trace(d_{ID})$ 成立(即两个密钥属于相同的解密密钥族)。

2. 安全性证明

定理 7.1　敌手在 IND-ID-CCA 游戏中的优势相对于以上的在 decisional truncated q-ABDHE 假设下的第三方权利受约束的基于身份的加密方案是可忽略的。

证明概述:这里使用的证明方法是严格遵照 Gentry 方案的 IND-ID-CCA 安全性证明方法进行的。这里只是简略叙述,主要的与其不同之处在于一个身份 ID 的解密密钥 d_{ID} 是怎样被分发的。在 Gentry 方案地证明中,PKG 自由地独立选取解密密钥 d_{ID} 并且将它发送给用户。事实上 PKG 使用了特定技术选择 $r_{ID,i}$,该技术依赖于 truncated q-ABDHE 问题给出的实例。本方案中 PKG 和用户 U 执行密钥产生协议,其中 $r_{ID,1}$ 是由他们双方共同确定的(分别经过 r,r' 次的选择),因此 PKG 没有能力独自产生 $r_{ID,1}$。

以上的问题能以如下方式解决。PKG 自己产生一个解密密钥 $d_{ID}=\{(r_{ID,i},h_{ID,i}):i\in\{1,2,3\}\}$,进而在密钥产生过程中,把 U 的输出作为上述的密钥。U 首先选择一个随机的 $r\in Z_p$ 并且将 $R=h_1^r$ 发送给 PKG,然后将一个 R 的离散对数知识的零知识证明给 PKG。这个证明系统的知识特性的证明隐含的提出存在一个知识提取器 Ext。在知识协议的证明过程中对 U 使用 Ext,PKG 能够以可忽略的概率提取离散对数 r(通过在协议执行过程中回卷 U)。此时 PKG 设定 $r'=rr_{ID,1}$。然后将 $(r',h'_{ID,1}=h_{ID,1}^r)$,$(r_{ID,2},h_{ID,2})$,$(r_{ID,3},h_{ID,3})$ 发送给 U。

用户 U 将计算 $r_{ID,1}=r'/r$,$h_{ID,1}=(h'_{ID,1})^{1/r}$。因此 PKG 已经成功迫使解密密

钥 d_{ID} 作为它提前选取的密钥。

定理 7.2 假设在 G_1 中计算离散对数是困难的，对于以上的第三方权利受约束的基于身份的加密方案，在 *FindKey* 游戏中敌手的优势是可以忽略的。

证明：在上述的 A-IBE 方案中，设有一个 PPT 算法 $\mathcal{A}$ 在发现密钥游戏中的优势为 ε。假设有一个挑战者 $\mathcal{B}$，有能力以 ε 的优势求解 G_1 中的离散对数。

$\mathcal{B}$ 运行算法 $\mathcal{A}$ 并从 $\mathcal{A}$ 处获得公开参数 $PK=(g_1,g_2,h_1,h_2,h_3)$ 和身份 ID。它接下来请求挑战者，将 h_1 传递给它并获得一个挑战 $R\in G_1$。$\mathcal{B}$ 的目的是去寻找 R 关于 h_1 的离散对数 r。

$\mathcal{B}$ 与 $\mathcal{A}$ 一起在密钥产生协议中获取 ID 的解密密钥过程如下：它将 R 发送给 $\mathcal{A}$ 同时必须给出一个 R 的离散对数知识的零知识证明。证明系统的零知识性暗示存在一个模仿者 S，该 S 能够以几乎可以忽略的概率成功地模仿协议（通过重新执行 $\mathcal{A}$）中 $\mathcal{A}$ 的想法。即使 $\mathcal{B}$ 没有 r 的知识，也要使用模仿者 S 去模仿需求的证明。$\mathcal{B}$ 接下来从 $\mathcal{A}$ 处接收串 $(r',h'_{ID,1}),(r_{ID,2},h_{ID,2}),(r_{ID,3},h_{ID,3})$。如前，$\mathcal{B}$ 运行一个密钥完整性检验，测试内容是判断 $e(h_{ID,i},g^{\alpha-ID})=e(h_ig^{-r_{ID,i}},g)$ 是否成立，其中 $i\in\{2,3\}$。如果 $i=1$，$\mathcal{B}$ 测试 $e(h'_{ID,i},g^{\alpha-ID})=e(Rg^{-r'},g)$ 是否成立。如果这些测试中的任何一个失败，那么 $\mathcal{B}$ 应该作为密钥产生协议中的主用户异常终止。

现在，$\mathcal{A}$ 以至少 ε 概率输出一个解密密钥 d'_{ID}（通过密钥完整性检验因此形式合法），则它的解密密钥族号为 n'_F。n'_F 等于密钥 d_{ID} 的解密密钥族号，其中 d_{ID} 被定义（但对于 $\mathcal{B}$ 是未知的）为 $((r'/r,(h'_{ID,1})^{1/r},(r_{ID,2},h_{ID,2}),(r_{ID,3},h_{ID,3}))$ 从 d'_{ID} 计算 n'_F 以后（通过对它跟踪），$\mathcal{B}$ 计算 $r=r'/n'_F$。$\mathcal{B}$ 输出 r 作为挑战 R 的离散对数（关于 h_1）并结束。

定理 7.3 对于以上在 Computational q-SDH 假设下的第三方权利受约束的基于身份的加密系统，敌手在计算新密钥游戏当中的优势是可以忽略不计的。

证明：设在以上的 A-IBE 假设中，有一个 PPT 算法 $\mathcal{A}$ 在计算新密钥游戏当中有优势 ε。需要说明如何构建一个挑战者 $\mathcal{B}$ 以相同的优势 ε 解决 Computational q-SDH 假设。$\mathcal{B}$ 的执行过程如下。

在这个证明中 $\mathcal{B}$ 的功能与 Gentry 的 IND-ID-CPA 证明方案中的挑战者的功能是相似的。$\mathcal{B}$ 请求挑战者并获得 q-SDH 问题的实例 $(g,g_1,g_2,\cdots,g_q)$ 作为输入，其中 $g_i=g^{(\alpha^i)}$。

$\mathcal{B}$ 随机产生 q 阶多项式 $f_i(x)\in Z_p[x](i\in\{1,2,3\})$。它用 $(g,g_1,g_2,\cdots,g_q)$ 计算 $h_i=g^{(\alpha^i)}$，并将公开参数 $PK=(g,g_1,h_1,h_2,h_3)$ 发送给算法 $\mathcal{A}$。

$\mathcal{B}$ 与 A 现在运行密钥产生协议，将解密密钥 $d_{ID^1},\cdots,d_{ID^q}$ 传递给由 $\mathcal{A}$ 适应性选择的身份 $ID^1,\cdots,ID^q$。对于一个身份 ID，$\mathcal{B}$ 执行密钥生成协议的过程如

下：如果 $ID=\alpha,\beta$ 使用 α 快速解决 q-SDH 问题。否则，设 $F_{ID,i}(x)$ 表示 $(q-1)$ 阶多项式 $F_{ID,i}(x)=(f_i(x)-f_i(ID))/(x-ID)$，$\mathcal{B}$ 计算解密密钥 $d_{ID}=\{(r_{ID,i},h_{ID,i}):i\in\{1,2,3\}\}$，其中 $r_{ID,i}=f_i(ID)$ 并且 $h_{ID,i}=g^{F_{ID,i}(\alpha)}$。如果 $h_{ID,i}=g^{(f_i(\alpha)-f_i(ID))/(\alpha-ID)}=(h_ig^{-f_i(ID)})^{1/(\alpha-ID)}$，则说明这是一个有效的私钥。此时在密钥生成协议的过程中 $\mathcal{B}$ 迫使 $\mathcal{A}$ 的输出作为私钥 d_{ID}（见定理 7.1 的证明）。

此时，对于一个身份 ID 满足 $trace(d^1_{ID})\neq trace(d^2_{ID})$，则 $\mathcal{A}$ 以最少 $\in$ 的概率输出两个解密密钥（通过了密钥完整性检验，因此形式合法）$d^1_{ID}=\{(r^1_{ID,i},h^1_{ID,i})\}$ 和 $d^2_{ID}=\{(r^2_{ID,i},h^2_{ID,i})\}(i\in\{1,2,3\})$。这也说明 $r^1_{ID,1}\neq d^2_{ID,1}$。$\mathcal{B}$ 接着计算

$$(h^1_{ID,1}/h^2_{ID,1})^{1/(r^2_{ID,1}-r^1_{ID,1})}=(h_1g^{-r^1_{ID,1}}/h_1g^{-r^2_{ID,1}})^{1/(r^2_{ID,1}-r^1_{ID,1})(\alpha-ID)}$$
$$=g^{1/(\alpha-ID)}$$

最终，$\mathcal{B}$ 输出 $(-ID,g^{1/(\alpha-ID)})$ 作为已知的 q-SDH 问题的实例的解决办法并结束。

7.3.2 基于 DBDH 假设的 A-IBE

这种第三方权利受约束的基于身份的加密方案是基于 DBDH 问题的。虽然这种构建方式不是非常有效并且每次解密都需要一些对操作。该问题是双线性映射群中的一个数学上的困难问题。Goyal 使用两个密码系统作为这种构建方式中的构造模块：分别是由 Waters 提出的基于身份的加密方案和由 Sahai 和 Waters 提出的模糊的基于身份的加密方案（FIBE）。

下面 1. 中的方案是使用从 Sahai 和 Waters 的构建方案（FIBE）中产生出来的 IBE 方案。在 FIBE 中，加密是通过一组属性完成的，而这组属性将由我们所设定的身份定义。另外，Goyal 在密文中加入了一组伪属性，通过密钥产生协议，用户在获得由他的身份定义的属性集的同时也获得了某个伪属性子集，这个子集能用来解密伪属性加密的部分密文。

1. 构建方式

与之前类似，G_1 是一个阶为素数 p 的双线性群，且设 g 是 G_1 的生成元。另外 $e:G_1\times G_1\rightarrow G_2$ 代表一个双线性映射。

用一个定长为 l_{ID} 的串表示一个身份（因为身份 $ID\in Z_p$，l_{ID} 是由 Z_p 中元素表示的所需的位数）。设 l_{sp} 是一个数，这个数由一个统计安全参数 κ_s 决定。设 $l=l_{ID}+l_{SP}$。定义以下集合：$S=\{1,\cdots,l\}$，$S_{ID}=\{1,\cdots,l_{ID}\}$，$S_{sp}=\{l_{ID}+1,\cdots,l\}$。用 ID_i 表示身份 ID 的第 i 位。构建方式如下：

Setup：运行 Waters 密码系统的初始化算法并且获得公共参数 PK_w 和主密钥 MK_w。此时，对于每个 $i\in S$，在 Z_p 中均匀随机的选择两个数 $t_{i,0}$ 和 $t_{i,1}$，这 $2l$ 个数都不同。还要在 Z_p 中均匀随机的选择一个数 y。

公开的公开参数是 $PK=(PK_w,PK_{sw})$，其中 $PK_{sw}=(\{(T_{i,j}=g^{t_{i,j}}):i\in S,j\in\{0,1\}\},Y=e(g,g)^y,g)$。

主密钥 $MK=(MK_w,MK_{sw})$，其中 $MK_{sw}=(\{(t_{i,j}):i\in S,j\notin\{0,1\}\},y)$。

Extract：密钥产生协议 PKG 和用户 U 之间的密钥产生协议（与身份 ID 有关）按如下方式进行：

（1）如果集合 $\{T_{i,j}:i\in S,j\in\{0,1\}\}$ 中的公开值不都是不同的，则 U 终止。

（2）PKG 按照 Waters 加密系统的密钥生成算法，使用 MK_w 为身份 ID 生成一个解密密钥 d_w。

（3）PKG 从 Z_p 中随机选出 l 个数 $r_1,\cdots,r_l$ 满足 $r_1+\cdots+r_l=y$。

（4）PKG 计算密钥组件 $d_{sw,i}=g^{r_i/t_{i,ID_i}}$（所有 $i\in S_{ID}$）并且将其发送给 U。它还要计算密钥组件 $d_{sw,i,j}=g^{r_i/t_{i,j}}$（所有 $i\in S_{sp},j\in\{0,1\}$）并将其存储。

（5）PKG 和 U 继续执行 l_{sp} 次 1/2 不经意传输协议。其中 PKG 充当了发送者，U 充当了接受者。在第 i 次执行过程中（其中 $i\in S_{sp}$），PKG 的独有的输入是部分密钥 $d_{sw,i,0}$ 和 $d_{sw,i,1}$ 且 U 独有的输入是一个随机选择的位 b_i。U 独有的输出为部分密钥 d_{sw,i,b_i}。

（6）U 计算 $d_{sw}=(\{d_{sw,i}\}_{i\in S_{ID}},\{b_i,d_{sw,i,b_i}\}_{i\in S_{sp}})$，并且对 d_{sw} 执行一个密钥完整性检验：

$$Y=\prod_{i\in S_{ID}}e(T_{i,ID_i},d_{sw,i})\prod_{i\in S_{sp}}e(T_{i,b_i},d_{sw,i,b_i})$$

如果以上的检验失败，则 U 终止。最终 U 计算它的解密密钥为 $d_{ID}=(d_w,d_{sw})$。

Encrypt：在一个身份 ID 下对信息 $m\in G_2$ 进行加密，需要将信息随机分为 m_1 和 m_2 两部分且满足 $m_1\oplus m_2=m$。现在选择一个随机值 $s\in Z_p$ 并计算密文 $c=(C_w,C_{sw})$。C_w 依据 Waters 密码系统的加密算法使用公开参数 PK_w 对带有 ID 的 m_1 进行加密，且 C_{sw} 通过如下计算得出

$$C_{sw}=(C'=m_2Y^s,C''=g^s,\{(C_i=T_{i,ID_i}^s):i\in S_{ID}\},\{(C_{i,j}=T_{i,j}^s):i\in S_{sp},j\in\{0,1\}\})$$

Decrype：使用解密密钥 $d_{ID}=(d_w,d_{sw})$ 对密文 $c=(C_w,C_{sw})$ 解密，但首先对 C_{sw} 执行密文完整性检测：

$$e(C_i,g)=e(T_{i,ID_i},C''),i\in S_{ID}$$

$$e(C_{i,j},g)=e(T_{i,j},C''),i\in S_{sp},j\in\{0,1\}$$

如果以上任何一个检测失败，输出“$\perp$”，表示检测失败；如果全部成立，则检测通过。很容易发现，这个检测能够确保 $\{(C_i=T_{i,ID_i}^s):i\in S_{ID}\}$，$\{(C_{i,j}=T_{i,j}^s):i\in S_{sp},j\in\{0,1\}\}$，其中 s 是关于 g 的 C'' 的离散对数。这确保了所有的无效密文都被拒绝。

如果密文完整性检验成功，使用 d_w 并且通过对 C_w 执行 Waters 密码系统的解密算法来恢复 m_1。m_2 则通过以下计算被恢复：

$$\begin{aligned} & C' / \prod_{i \in S_{ID}} e(C_i, d_{sw,i}) \prod_{i \in S_{sp}} e(C_{i,b_i}, d_{sw,i,b_i}) \\ &= m_2 e(g,g)^{sy} / \prod_{i \in S_{ID}} e(g^{st_{i,ID_i}}, g^{r_i/t_{i,ID_i}}) \prod_{i \in S_{sp}} e(g^{st_{i,b_i}}, g^{r_i/t_{i,b_i}}) \\ &= m_2 e(g,g)^{sy} / \prod_{i \in S} e(g,g)^{sr_i} \\ &= m_2 \end{aligned}$$

最后，输出 $m = m_1 \oplus m_2$。

Trace：这个算法需要一个形式合法的解密密钥 $d_{ID} = (d_w, d_{sw})$，其中组件 $d_{sw} = (\{d_{sw,i}\}_{i \in S_{ID}}, \{b_i, d_{sw,i,b_i}\}_{i \in S_{sp}})$，并且输出解密密钥族号 $n_F = b_{l_{ID}+1} \circ b_{l_{ID}+2} \circ \cdots \circ b_l$，其中 $\circ$ 表示连接符。

2. 安全性证明

定理 7.4　对于以上可追踪的基于身份的加密方案，在 decisional BDH 假设下，IND-ID-CPA 游戏中的敌手的优势是可以忽略的。

上述定理由 Waters 构建的 IND-ID-CPA 方案可轻易得出。如果有敌手打破了本方案的 IND-ID-CPA 安全性，那么他也就可以打破 Waters 构建的 IND-ID-CPA 安全性。本章中我们将省略这些细节。

与 Water 方案相似，它可能通过小的修改使用 Canetti，Halevi 和 Katz 的方法去获得 IND-ID-CCA 安全性，也可以使用其他的方法获得好的效率。

定理 7.5　假设基本的 1/2 不经意传输协议是安全的，对于以上的基于可追踪身份的加密方案，敌手在 FindKey 游戏中的优势是可以忽略的。

在密钥产生的阶段中，$\mathcal{A}$ 和挑战者将经历 l_{sp} 次 1/2 不经意传输阶段，其中挑战者选择 l_{sp} 位 $b_{l_{ID}+1}, b_{l_{ID}+2}, \cdots, b_l$ 并且获得与密钥相对应的部分。现在如果 $\mathcal{A}$ 能够从相同的解密密钥族中输出一个解密密钥，这说明它能够成功地猜出位串 $b_{l_{ID}+1} \circ b_{l_{ID}+2} \circ \cdots \circ b_l$ 在不经意传输阶段被使用。因此，很容易构建一个挑战者 $\mathcal{B}$ 去破坏基本的不经意传输协议的安全性。

定理 7.6　对于以上的可追踪的基于身份的加密方案，在 decisional BDH 假设下，在 *Selective-ID ComputeNewKey* 游戏中敌手的优势是可以忽略的。

证明：为了使证明过程更清晰，我们将其分成两个阶段。第一阶段，提出一个假设与 computational Diffie-Hellman 假设非常类似，称作 computational MDH 假设。由于 computational MDH 必然包含 decisional（事实上是 computational）BDH。在第二阶段，在 computational MDH 假设下证明在 *Selective-ID ComputeNewKey* 游戏中敌手的优势是可以忽略的。

Computational MDH 假设是在已知元组(g^a,g^b)的情况下,没有 PPT 的算法能够以不可忽略的优势计算 $g^{a/b}$。已知一个解决 MDH 问题的预言机 O,我们说明了怎样构建一个预言机 P 用来解决 decisional BDH 假设。P 把 BDH 实例($A=g^a$,$B=g^b$,$C=g^c$,Z)作为输入并且对 O 进行 3 次请求如下:第一次传递元组(A,B)并获得结果 D_1;接下来传递元组(D_1,A)并获得元组 D_2;最终,传递元组(D_2,A)获得结果 D。很容易发现如果有 3 次询问,O 都返回正确的结果 $D=g^{ab}$。P 接下来检查 $Z=e(D,C)$是否成立,如果检查失败返回 0,否则返回 1。因此,如果 O 的成功率是 ε,则 P 的成功率为 ε^3。

设在以上的 A-IBE 构建中有一个 PPT 算法 $\mathcal{A}$ 在 *Selective-ID ComputeNewKey* 游戏中有不可忽略的优势 ε。我们将说明如何构建一个能够以不可忽略的优势 $\varepsilon/2l_{sp}$解决 computational MDH 假设的挑战者 $\mathcal{B}$。$\mathcal{B}$ 如下继续执行。将 MDH 问题的实例($A=g^a$,$B=g^b$)作为输入。它请求 $\mathcal{A}$ 并获取身份 ID,$\mathcal{A}$ 愿意对身份 ID 做新的密钥计算。$\mathcal{B}$ 建立公共参数如下:运行 Waters 密码系统的初始化算法并获得公共参数 PK_w 和主密钥 MK_w。对于任意 $i\in S$ 均匀随机地从 Z_p 中选择两个数 $t'_{i,0}$和 $t'_{i,1}$。对于任意 $i\in S_{ID,j}\in\{0,1\}$,如果 $j=ID_i$,定义 $t_{i,j}=bt'_{i,j}$(尽管 b 是未知的),否则定义 $t_{i,j}=t'_{i,j}$。现在选择一个随机的索引 $ind\in S_{sp}$和一个随机位 $indbit\in\{0,1\}$。对于任意 $i\in S_{sp}$,$j\in\{0,1\}$,如果 $i=ind$ 且 $j=indbit$,定义 $t_{i,j}=t'_{i,j}$,否则定义 $t_{i,j}=bt'_{i,j}$。设 $bit(t_{i,j})$代表一个函数,该函数负责判断:如果 $t_{i,j}=t'_{i,j}$,则结果是 0,否则结果为 1。

公共的公开参数 $PK=(PK_w,PK_{sw})$,其中 $PK_{sw}=(\{(T_{i,j}=g^{t_{i,j}}):i\in S,j\in\{0,1\}\})$,$Y=e(g,g)^a$,$g)$。

$\mathcal{B}$ 现在与 $\mathcal{A}$(可能是多次)一起运行密钥产生协议。由 $\mathcal{A}$ 适应选择的身份 $ID^1,\cdots,ID^q$,$\mathcal{B}$ 计算并传递解密密钥 $d_{ID^1},\cdots,d_{ID^q}$。

对于一个身份 $ID'\neq ID$,$\mathcal{B}$ 执行密钥生成协议如下:选择一个任意的数 $k\in S_{ID}$使得 $ID'_k\neq ID_k$。对于所有的 $i\in S,i\neq k$,选择随机的 r'_i并定义 $r_i=br'_i$(注意既然 b 是未知的,那么 r_i 对于 $\mathcal{B}$ 也是未知的)。$\mathcal{B}$ 计算部分解密密钥如下:

对于所有 $i\in S_{ID},i\neq k$,如果 $bit(t_{i,ID'_i})=0$(t_{i,ID'_i}在这个例子中是已知的),则 $d_{sw,i}=\begin{cases}g^{r_i/t_{i,ID_i'}}\\ g^{r'_i/t'_{i,ID_i'}}\end{cases}$。

否则,对于 $i=k$,则 $d_{sw,i}=(g^a/g^{r_1+\cdots+r_{i-1}+r_{i+1}+\cdots+r_l})^{1/t_{i,ID'_i}}$($t_{i,ID'_i}$在这个例子中是已知的)。

对于所有 $i\in S_{sp},j\in\{0,1\}$,如果 $bit(t_{i,j})=0$,则 $d_{sw,i,j}=\begin{cases}g^{r_i/t_{i,j}}\\ g^{r'_i/t'_{i,j}}\end{cases}$。

否则,很容易证实,以上的密钥是被正确组建的。有了这些密钥,$\mathcal{B}$ 可顺利

完成密钥产生协议的剩余部分。算法 $\mathcal{A}$ 将解密密钥 $d_{ID'}=d_w,d_s w$ 作为输出。

对于身份 ID 本身，密钥产生协议的内容将涉及更加细微的问题。对于所有 $i\in S,i\neq ind$，随机选择 r_i' 并定义 $r_i=br_i'$（注意，由于 b 是未知，则对于 $\mathcal{B}$，r_i 是未知的）。$\mathcal{B}$ 计算部分解密密钥如下：

对于所有的 $i\in S_{ID}$，$d_{sw,i}=g^{r_i'/t_{i,ID_i}}$（$t_{i,ID_i}$ 对于所有 i 是未知的）。

对于 $i=ind,j=indbit$，$d_{sw,i,j}=(g^a/g^{r_1+\cdots+r_{i-1}+r_{i+1}+\cdots+r_l})^{1/t_{i,j}}$（$t_{i,j}$ 在这个例子中是已知的）。

对于所有的 $i\in S_{sp},i\neq ind,j\in\{0,1\}$，如果 $bit(t_{i,j})=0$，则 $d_{sw,i,j}=\begin{cases}g^{r_i'/t_{i,j}}\\ g^{r_i'/t_{i,j}'}\end{cases}$。

否则，再一次很容易地证明以上的密钥是被正确组建的。注意这里遗漏了一个部分解密密钥：$d_{sw,ind,\neg indbit}$，算法 $\mathcal{A}$ 将不会在 1/2 不经意传输阶段内对它进行询问（用对 $d_{sw,ind,indbit}$ 的询问代替）。$\mathcal{B}$ 为这个密钥设定一些随机值，并同协议的剩余部分一起继续执行。由 $\mathcal{A}$ 选择的位 b_{ind} 有 1/2 的几率（因为 $indbit$ 是随机选取的）等同于 $indbit$ 并且因此 $\mathcal{A}$ 获得一个有效的解密密钥 d_{ID}。如果不是这种情况，$\mathcal{B}$ 终止并且输出失败。

现在，$\mathcal{A}$ 以最少为 ε 的概率，输出两个来自不同的解密密钥族的解密密钥（通过了完整性检验，因此是形式合法的）d_{ID}^1 和 d_{ID}^2。这意味着至少存在一个 $i\in S_{sp}$ 使得满足 $b_i^1\neq b_i^2$。$ind=i$（由于 ind 是随机选取的）的概率最少为 $1/l_{sp}$。如果不是这样的话，$\mathcal{B}$ 终止并输出 $Fail$。否则 k 满足 $b_{ind}^k=\neg indbit$。

对于所有的 $i\in S_{ID}$，$bit(t_{i,ID_i})=1$ 且对于所有的 $i\in S_{sp}$，$bit(t_{i,b_i^k})=1$。$\mathcal{B}$ 计算：

$$\begin{aligned}\prod_{i\in S_{ID}}(d_{sw,i}^k)^{t_{i,ID_i}'}\prod_{i\in S_{sp}}(d_{sw,i,b_i^k}^k)^{t_{i,b_i^k}'}&=\prod_{i\in S_{ID}}(g^{r_i'/bt_{i,ID_i}'})^{t_{i,ID_i}'}\prod_{i\in S_{sp}}(g^{r_i'/bt_{i,b_i^k}'})^{t_{i,b_i^k}'}\\&=\prod_{i\in S}g^{r_i'/b}\\&=g^{a/b}\end{aligned}$$

$\mathcal{B}$ 输出 $g^{a/b}$ 作为已知的 computational MDH 问题的解答并结束。

7.4　Xu 等人的通用 A-IBE 方案

7.4.1　构建方式

对于任意取定的且具有语义安全性的 IBE 方案 I，Xu 等人的通用 A-IBE 方案构造如下：

令 G_1 是具有对运算的大素数 p 阶群，g 为其生成元；令群 G_1 上的对运算为

$e:G_1\times G_1\to G$，令 $\sum=\{1,\cdots,n\}$ 是大小为 n 的字母表；令身份信息 $ID\in\sum^{l_{ID}}$ 为身份信息的长度，ID_i 表示 ID 的第 i 个字母；令 l_s 是关于安全参数 k 的多项式。令 $l=l_{ID}+l_s$，$S_{ID}=\{l_{ID}+1,\cdots,l\}$。

Setup-uA 算法：取唯一的输入——安全参数 k；运行 I 的 $Setup(k)$ 算法，得到 I 的公开参数 *PK-I* 和主密钥 *MK-I*；随机选取 $y\in Z_p$ 和 $n\times l$ 阶主矩阵

$$\boldsymbol{MM}=\begin{pmatrix}t_{1,1} & \cdots & t_{1,l}\\ \vdots & & \vdots\\ t_{n,1} & \cdots & t_{n,l}\end{pmatrix}$$

其中所有的 $t_{i,j}\in Z_p$ 均不相同；相应地，计算公开矩阵

$$\boldsymbol{PM}=\begin{pmatrix}T_{1,1}=g^{t_{1,1}} & \cdots & T_{1,l}=g^{t_{1,l}}\\ \vdots & & \vdots\\ T_{n,1}=g^{t_{n,1}} & \cdots & T_{n,l}=g^{t_{n,l}}\end{pmatrix}$$

发布公开参数 $PK=\{PK\text{-}I,PK\text{-}A\}$，其中 $PK\text{-}A=\{\boldsymbol{PM},g^y\}$，保密主密钥 $MK=\{MK\text{-}I,MK\text{-}A\}$，其中 $MK\text{-}A=\{\boldsymbol{MM},y\}$。该方案的明文空间可以合理地认为是群 G_1。

KeyGeneration 协议：该协议由 PKG 和用户 U（身份信息为 ID）按如下过程实施：

（1）PKG 随机地选取 l 个数：$\{r_1,\cdots,r_l\}\in(Z_p)^l$，且使得 $r_1+\cdots+r_l=y$ 成立。

（2）对任意的 $i\in S_{ID}$：PKG 从主矩阵 $\boldsymbol{MM}$ 中选取元素 $t_{ID_i,i}$，计算并返回 $r_i/t_{ID_i,i}$ 给 U。

（3）对任意的 $i\in S_s$：PKG 计算 n 个元素：$\{r_i/t_{1,i},\cdots,r_i/t_{n,i}\}$，并作为其运行 OT_n^1 协议的私有输入，其中 $\{t_{1,i},\cdots,t_{n,i}\}$ 来自于主矩阵 $\boldsymbol{MM}$；U 秘密地选取 $d_i\in\sum$，并将其作为其运行 OT_n^1 协议的私有输入；PKG 和 U 运行 OT_n^1 协议，使得 U 仅得到秘密 $r_i/t_{d_i,i}$，且 PKG 无法知道 d_i。

（4）U 计算其私钥 $d_A=\{\{r_i/t_{ID_i,i}\}_{i\in S_{ID}},\{d_i,r_i/t_{d_i,i}\}_{i\in S_s}\}$，并且进行密钥有效性检测，即检测

$$g^y=\prod_{i\in S_{ID}}(T_{ID_i,i})^{r_i/t_{ID_i,i}}\prod_{i\in S_s}(T_{d_i,i})^{r_i/t_{d_i,i}}$$

若等式不成立，则 U 退出。

（5）对于 U 的身份信息 ID，PKG 根据 I 的参数 $\{PK\text{-}I,MK\text{-}I\}$，运行 I 的 *Extract* 算法计算其部分私钥 d_I 并返回给 U，最后 U 将 $d_{ID}=\{d_I,d_A\}$ 作为其完整的私钥。

Encrypt-uA 算法：取身份信息 ID、公开参数 PK 和明文 $m\in G_1$ 作为输入，该随机化算法按如下过程计算密文 $c=\{C_1,C_2\}$：

（1）随机选取 $m_1 \in G_1$，令 $m = m_1 \times m_2$，其中 $m_2 \in G_1$。

（2）运行 I 的 *Encrypt* 算法，计算 $C_1 = Encrypt(ID; PK\text{-}I; m_1)$。

（3）C_2 是 m_2 的密文且 $C_2 = (C'' = g^s, C^1 = g^{sy} \cdot m_2, \{C'_i = (T_{ID_i,i})^s\}_{i \in S_{ID}}, \{C_{i,j} = (T_{i,j})^s\}_{i \in \sum, j \in S_s})$，其中 s 在 Z_p 中随机选取。

Decrypt-uA 算法：该确定性算法以私钥 d_{ID}、公开参数 PK 和密文 $c = \{C_1, C_2\}$ 作为输入，分别通过解密 C_1 和 C_2，计算出 m_1 和 m_2，其中 $m_1 = Decrypt(d_I; PK\text{-}I; C_1)$（*Decrypt* 算法是 I 的解密算法）。C_2 的解密过程如下：

（1）首先运行密文有效性检测，即检测 $\forall i \in S_{ID}, e(C'_i, g) = e(C'', T_{ID_i,i})$；$\forall i \in \sum$ 和 $j \in S_s, e(C'_{i,j}, g) = e(C'', T_{i,j})$，若有任意的一个等式不成立，则输出“⊥”（该符号在文中表示算法出现异常并停机）。由于通用 A-IBE 方案的语义安全性完全继承于其选取的 IBE 方案的语义安全性，因此此处的密文有效性检测并不关心整个的密文 C_2，只关心其最后的两个部分，即（$\{C'_i\}_{i \in S_{ID}}, \{C_{i,j}\}_{i \in \sum, j \in S_s}$）的有效性（显然，在 CCA 安全性下，此做法无法保证语义安全性，因此进一步地说明 C_2 并不需要在意语义安全性问题）。而此处的密文有效性检测主要是为了保证：即使敌手可以适应性地选择密文进行解密询问，他也无法知道 d_{ID} 中有关 d_i 的信息；另一方面，该密文有效性检测中的对运算可以减少为两次。

（2）计算 m_2 的方式如下：

$$\frac{C'}{\prod_{i \in S_{ID}} (C'_i)^{r_i / t_{ID_i,i}} \prod_{i \in S_s} (C'_{d_i,i})^{r_i / t_{d_i,i}}} = \frac{g^{sy} \cdot m_2}{\prod_{i \in S_{ID}} g^{sr_i} \prod_{i \in S_s} g^{sr_i}} = m_2$$

最后输出 $m = m_1 \cdot m_2$。

Trace 算法：取私钥 d_{ID} 作为输入，该确定算法输出 $Trace(d_{ID}) = d_{l_{ID}+1} \| \cdots \| d_l$，即私钥的特征值为所有 d_i 的串联。

7.4.2　安全性分析

本节给出安全性定义 *FindKey game* 和 *ComputeNewKey game* 下，新的通用 A-IBE 方案的安全性证明。

定理 7.7　假设 OT_n^1 协议是安全的，则在安全性定义 *FindKey game* 下，敌手成功攻破新的通用 A-IBE 方案的优势可忽略。

证明：显然可以看出，若敌手可以生成新的私钥，且和原有私钥 d_{ID} 具有相同的特征信息，则该敌手已经成功的猜测了 $d_{l_{ID}+1} \| \cdots \| d_l$ 而且由于在新的通用 A-IBE 方案的 *KeyGeneration* 协议中，所有 $d_{l_{ID}+1} \| \cdots \| d_l$ 的 d_i 均由用户 U 秘密选取，且仅在 l_s 次 OT_n^1 协议的运行中作为 U 的秘密输入使用，因此该敌手在成功猜测了 $d_{l_{ID}+1} \| \cdots \| d_l$ 的同时，也就破解了 OT_n^1 协议的安全性。但是这和 OT_n^1 协议是安全的假设相矛盾，因此敌手无法成功地猜测 $d_{l_{ID}+1} \| \cdots \| d_l$，也就无法破坏

新的通用 A-IBE 方案的 *FindKey game* 安全性，即在安全性定义 *FindKey game* 下，敌手成功攻破新的通用 A-IBE 方案的优势可忽略。

定理 7.8 假设 DL 假设成立，则在安全性定义 *ComputeNewKey game* 下，敌手成功攻破新的通用 A-IBE 方案的优势可忽略。

证明：假设存在敌手 $\mathcal{A}$ 可以以不可忽略的概率有效地生成挑战 *ID* 的两个有效的私钥 d_{ID}^1 和 d_{ID}^2，且 $Trace(d_{ID}^1) \neq Trace(d_{ID}^2)$，那么可以构造一个有效的算法 $\mathcal{B}$ 以不可忽略的概率求解 *DL* 问题。

令群 G_1 上的 DL 问题为：给定 g^a，其中 a 在 Z_p 中随机选取，计算 a。算法 $\mathcal{B}$ 按敌手 $\mathcal{A}$ 的不可忽略优势如下求解 DL 问题：

Setup：算法 $\mathcal{B}$ 运行新的通用 A-IBE 方案的 *Setup-uA* 算法，生成公开参数 $PK = \{PK\text{-}I, PK\text{-}A\}$ 和主密钥 $MK = \{MK\text{-}I, MK\text{-}A\}$，其中

$$MK\text{-}A = \{\boldsymbol{MM}; y\}$$

$$\boldsymbol{MM} = \begin{pmatrix} t_{1,1} & \cdots & t_{1,l-1} & t_{1,l} \\ \vdots & & \vdots & \vdots \\ t_{n-1,1} & \cdots & t_{n-1,l-1} & t_{n-1,l} \\ t_{n,1} & \cdots & t_{n,l-1} & Null \end{pmatrix}$$

$$PK - A = \{\boldsymbol{PM}, g^y\}$$

$$\boldsymbol{PM} = \begin{pmatrix} T_{1,1} = g^{t_{1,1}} & \cdots & T_{1,l} = g^{t_{1,l}} \\ \vdots & & \vdots \\ T_{n,1} = g^{t_{n,1}} & \cdots & T_{n,l} = g^a \end{pmatrix}$$

注意：和真实的新的通用 A-IBE 方案相比，该阶段唯一的不同是主矩阵 $\boldsymbol{MM}$ 的第 n 行、l 列元素；且除此之外，所有的参数和真实的新的通用 A-IBE 方案具有相同的分布，即不可区分。最后算法 $\mathcal{B}$ 公布 $PK = \{PK\text{-}I; PK\text{-}A\}$ 给 $\mathcal{A}$。

KeyGeneration：该阶段敌手可以通过与算法 $\mathcal{B}$ 运行 *KeyGeneration* 协议，询问到任意用户的私钥。对于敌手 $\mathcal{A}$ 询问的任意身份信息 *ID*，算法 $\mathcal{B}$ 的处理过程如下：

(1) 算法 $\mathcal{B}$ 随机地在 Z_p 中选取 $r_1, \cdots, r_l$，且有 $r_1 + \cdots + r_l = y$。

(2) 对任意的 $i \in S_{ID}$，算法 $\mathcal{B}$ 计算并返回 $r_i / t_{ID_i,i}$ 给 $\mathcal{A}$。

(3) 对任意的 $i \in S_s$ 和 $i \neq l$，敌手 $\mathcal{A}$ 秘密选取 $d_i \in \sum$ 作为其私有输入，算法 $\mathcal{B}$ 秘密计算 $\{r_i / t_{1,i}, \cdots, r_i / t_{n,i}\}$ 作为其私有输入，然后共同运行 OT_n^1 协议，使得 $\mathcal{A}$ 仅得到 $r_i / t_{d_i,i}$ 且算法 $\mathcal{B}$ 无法知道 d_i。

(4) 当 $i = l$ 时，与上一步唯一的不同是：算法 $\mathcal{B}$ 运行 OT_n^1 协议的私有输入为 $\{r_l / t_{1,l}, \cdots, r_l / t_{n-1,l}, r_l\}$，而其他过程完全相同。

(5) 上述过程结束后,敌手 $\mathcal{A}$ 得到部分私钥 $d_{\mathcal{A}}$,且

$$d_{\mathcal{A}} = \{\{r_i/t_{ID_i,i}\}_{i\in S_{ID}}, \{d_i, r_l/t_{d_l,l} : d_l \neq n\} or \{d_i, r_l : d_l = n\}\}$$

敌手 $\mathcal{A}$ 运行密钥有效性检测,且该检测分为以下两种情况:

情况 1:若 $d_l \neq n$,则显然 $d_{\mathcal{A}}$ 总是能通过检测。

情况 2:若 $d_l = n$,则 $d_{\mathcal{A}}$ 仅在 $a = 1$ 时可以通过猜测,且由于 $a = 1$ 的概率可忽略,因此此时 $d_{\mathcal{A}}$ 仅以可忽略的概率通过猜测,即此时 $d_{\mathcal{A}}$ 几乎总是无法通过检测。

(6) 若 $d_{\mathcal{A}}$ 未能通过密钥有效性检测,则敌手 $\mathcal{A}$ 和算法 $\mathcal{B}$ 均退出。

(7) 算法 $\mathcal{B}$ 运行 I 的 *Extract* 算法,生成身份信息 ID 的部分私钥 d_I 给敌手 $\mathcal{A}$。敌手 $\mathcal{A}$ 最后得到 ID 的完整的私钥 $d_{ID} = \{d_I, d_{\mathcal{A}}\}$。

NewKeyGeneration:敌手 $\mathcal{A}$ 对其选取的挑战 ID,以不可忽略的概率生成两个有效的私钥 d_{ID}^1 和 d_{ID}^2,且 $Trace(d_{ID}^1) \neq Trace(d_{ID}^2)$. 对任意的 $k \in \{1,2\}$,令

$$d_{ID}^k = \{d_I^k, d_{\mathcal{A}}^k = \{\{d_{\mathcal{A},i}^k\}_{i\in S_{ID}}, \{d_i^k, d_{\mathcal{A},i}^k\}_{i\in S_s}\}\}$$

则对给定的 g^a,算法 $\mathcal{B}$ 计算 a 的过程如下:

(1) 对任意的 $k \in \{1,2\}$,算法 $\mathcal{B}$ 运行密钥有效性检测过程,检测 d_{ID}^k 的有效性;若 d_{ID}^k 无效,则算法 $\mathcal{B}$ 退出。

(2) 对任意的 $k \in \{1,2\}$,若 d_{ID}^k 均有 $d_l^k \neq n$,则算法 $\mathcal{B}$ 退出。否则,至少存在一个 $d_{ID}^k \in \{d_{ID}^1, d_{ID}^2\}$ 有 $d_l^k = n$,更进一步地,若该 d_{ID}^k 中 $d_{\mathcal{A},l}^k = 0$,则算法 $\mathcal{B}$ 也退出。若算法 $\mathcal{B}$ 没有退出,则令 $d_{ID}^k \in \{d_{ID}^1, d_{ID}^2\}$ 且满足 $d_l^k = n$ 和 $d_{\mathcal{A},l}^k \neq 0$。算法 $\mathcal{B}$ 再按如下步骤计算 a:

(1) 对任意的 $i \in \{1,\cdots,l-1\}$,由于已知 $\{t_{ID_i,i}\}_{i\in S_{ID}} \cup \{t_{d_i^k,i}\}_{i\in S_s - \{l\}}$,则算法 $\mathcal{B}$ 为任意的 $i \in S_{ID}$ 计算 $r_i^k = (d_{\mathcal{A},i}^k)^{t_{ID_i,i}}$,为任意的 $i \in S_s - \{l\}$ 计算 $r_l^k = (d_{\mathcal{A},i}^k)^{t_{d_i^k,i}}$。

(2) 然后由于已知 y,算法 $\mathcal{B}$ 计算 $r_l^k = y - (r_1^k + \cdots + r_{l-1}^k)$。

(3) 由于 d_{ID}^k 通过了密钥有效性检测且其 $d_l^k = n$,则有 $(T_{n,l})^{d_{\mathcal{A},l}^k} = g^{r_l^k}$ 成立。进一步地,由于公开矩阵 $\boldsymbol{PM}$ 中 $T_{n,l} = g^a$,即 $g^{a\cdot d_{\mathcal{A},l}^k} = g^{r_l^k}$,显然可以推出 $a \cdot d_{\mathcal{A},l}^k = r_l^k$。因此算法 $\mathcal{B}$ 可以通过计算 $r_l^k \cdot (d_{\mathcal{A},l}^k)^{-1}$,有效求解 a。

以上描述即为算法 $\mathcal{B}$ 的整个过程。显然算法 $\mathcal{B}$ 的正确性是很容易验证的,并且可以在有效时间内停止。下面将分别简要分析:在算法 $\mathcal{B}$ 不退出的条件下,其构造的环境和真实的新的通用 A-IBE 方案不可区分以及算法 $\mathcal{B}$ 成功求解 DL 问题的概率。

在算法 $\mathcal{B}$ 的初始化阶段,所有的公开参数和真实的新的通用 A-IBE 方案的 *Setup-uA* 算法的输出具有相同的分布;其 *KeyGeneration* 阶段,若算法 $\mathcal{B}$ 没有退出(即敌手 $\mathcal{A}$ 成功地通过了私钥有效性检测,且其运行 OT_n^1 协议的私有输入 d_l 不等于 n),则显然有算法 $\mathcal{B}$ 发送给敌手 $\mathcal{A}$ 的响应数据均和真实环境下的

KeyGeneration 协议具有相同分布。因此，只要算法 $\mathcal{B}$ 没有退出，则其构造的环境和真实的新的通用 A-IBE 方案的环境不可区分。

算法 $\mathcal{B}$ 成功求解 DL 问题的概率主要由算法 $\mathcal{B}$ 不退出的概率确定。下面将分别计算 *KeyGeneration* 阶段和 *NewKeyGeneration* 阶段中，算法 $\mathcal{B}$ 退出的概率。

KeyGeneration：根据算法 $\mathcal{B}$ 的构造可以看出，每一次的私钥生成过程和其他已生成的私钥是相互独立的，甚至同一个用户的不同私钥也是相互独立的。因此每一次私钥的生成过程中，由敌手 $\mathcal{A}$ 选择的 $d_l \neq n$ 的概率为 $(1-1/n)$；那么对于 q_{ID} 次私钥的生成过程而言，算法 $\mathcal{B}$ 不退出的概率为 $(1-1/n)^{q_{ID}}$。

NewKeyGeneration：在安全性定义 *ComputeNewKey game* 下，令敌手 $\mathcal{A}$ 以不可忽略的概率 ε 有效地计算出挑战 *ID* 的两个有效的私钥 d_{ID}^1 和 d_{ID}^2，且有 $Trace(d_{ID}^1) \neq Trace(d_{ID}^2)$。假设该阶段算法 $\mathcal{B}$ 不退出，则该事件的成立等价于下面 3 个事件同时成立，分别如下：

事件 1：敌手 $\mathcal{A}$ 生成的私钥 d_{ID}^1 和 d_{ID}^2 通过密钥有效性检测，且该事件成功的概率为 ε。

事件 2：至少存在一个私钥 $d_{ID}^k \in \{d_{ID}^1, d_{ID}^2\}$ 满足 $d_l^k = n$。由于所有的私钥生成是相互独立的，且公开矩阵 *PM* 中所有元素具有相同分布，则该事件的成功概率为 $1/n$。

事件 3：在事件 2 成立的基础上，d_{ID}^k 的 $d_{\mathcal{A},l}^k$ 不等于 0。由于 $\{d_{\mathcal{A},i}^k\}_{i\in\{1,\cdots,l\}}$ 中至少有一个 $d_{\mathcal{A},l}^k$ 不等于 0，且公开矩阵 *PM* 中所有元素具有相同分布，则该事件的成功概率为 $1/l$。

因此，算法 $\mathcal{B}$ 不退出的概率为 $(1-1/n)^{q_{ID}}\frac{\varepsilon}{n\cdot l}$。显然有，当 $n=q_{ID}$ 时，该概率最低，即 $(1-1/n)^{q_{ID}}\frac{\varepsilon}{n\cdot l}\approx\varepsilon/(e\cdot q_{ID}\cdot l)$，因此算法 $\mathcal{B}$ 不退出的概率不可忽略，也就是说，算法 $\mathcal{B}$ 可以以不可忽略的概率求解 DL 问题。显然上述结论和 DL 假设成立相矛盾，因此在安全性定义 *ComputeNewKey game* 下，不存在敌手能够以有效的和不可忽略的概率成功攻破新的通用 A-IBE 方案。

参 考 文 献

[1] Gentry C. Practical identity-based encryption without random oracles, Lecture notes in computer science, 2006, Vol. 4004: 445-464.

[2] Abdalla M, Bellare M, Catalano D. Searchable encryption revisited: consistency properties, relation to anonymous IBE and extensions, Lecture notes in computer science, 2006, In Advances in 2005, Vol. 3621: 205-222.

[3] Boneh D, Boyen X. Efficient selective-ID identity based encryption without random oracles,

Lecture notes in computer science,2004, Vol. 3027:223-238.

[4] Boneh D,Boyen X. Secure identity based encryption without random oracles, Lecture notes in computer science, 2004, Vol. 3152:443-459.

[5] Boneh D, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext, Lecture notes in computer science,2005, Vol. 3494:440-456.

[6] Boneh D,Crescenzo C D,Ostrovsky R. Public key encryption with keyword search, Lecture notes in computer science,2004, Vol. 3027:506-522.

[7] Boneh D,Franklin M. Identity based encryption from the weil pairing, Lecture notes in computer science,2001, Vol. 2139:213-229.

[8] Boneh D, Gentry C,Waters B. Collusion-resistant broadcast encryption with short ciphertexts and private keys, Lecture notes in computer science,2005, Vol. 3621:258-275.

[9] Boneh D,Katz J. Improved efficiency for CCA-secure cryptosystems built using identity based encryption, Lecture notes in computer science, 2005, Vol. 3376:87-103.

[10] Boneh D, Lynn B,Shacham H. Short signatures from the weil pairing, Lecture notes in computer science, 2001, Vol. 2248:514-532.

[11] Boyen X, Mei Q, Waters B. Direct chosen ciphertext security from identity based techniques, In Proc. of ACM CCS,2005:320-329.

[12] Canetti R,Halevi S,Katz J. A forward-secure public-Key encryption scheme, Lecture notes in computer science,2003, Vol. 2656:255-271.

[13] Canetti R, Halevi S, Katz J. Chosen-ciphertext security from identity-based encryption, Lecture notes in computer science,2004, Vol. 3027:207-222.

[14] Cramer R,Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attacks, Lecture notes in computer science,1998, Vol. 1462:13-25.

[15] Cramer R,Shoup V. Signature schemes based on the strong RSA assumption, In Proc. of ACM CCS,1999:46-51.

[16] Dodis Y. Efficient construction of distributed verifiable random functions, Lecture notes in computer science, 2002, Vol. 2567:1-17.

[17] Dodis Y,Yampolskiy A. A verifiable random function with short proofs and keys, Lecture notes in computer science, 2005, Vol. 3386:416-431.

[18] Gentry C,Silverberg A. Hierarchical ID-based cryptography, Lecture notes in computer science, 2002, Vol. 2501:548-566.

[19] Horwitz J, Lynn B. Toward hierarchical identity-Based encryption, Lecture notes in computer science, 2002, Vol. 2332:466-481.

[20] Katz J, Wang N. Efficiency improvements for signature schemes with tight security reductions, In Proc. of ACM CCS, 2003:155-164.

[21] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme, Lecture notes in computer science, 2004, Vol. 3152:426-442.

[22] Shamir A. Identity-based cryptosystems and signature schemes, Lecture notes in computer

science, 1984, Vol. 196:47-53.

[23] Shoup V. Lower bounds for discrete logarithms and related problems, Lecture notes in computer science, 1997, Vol. 1233:256-266.

[24] Waters B. Efficient identity-Based encryption without random oracles, Lecture notes in computer science, 2005, Vol. 3494:114-127.

[25] Barreto P. Kim H, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems, Lecture notes in computer science,2002, Vol. 2002:354-369.

[26] Bellare M, Desai A, Pointcheval D, Rogaway P. Relations among notions of security for public-key encryption schemes, Lecture notes in computer science, 1998, Vol. 1462:26-45.

[27] Boneh D. The decision Diffie-Hellman problem, Lecture notes in computer science, 1998, Vol. 1423:48-63.

[28] Bellare M. Boldyreva A, Micali S. Public-key encryption in a multi-User setting: security proofs and improvements, Lecture notes in computer science, 2000, Vol. 1807:259-274.

[29] Cocks C. An identity based encryption scheme based on quadratic residues, Lecture notes in computer science, 2001, Vol. 2260:360-363.

[30] Coron J. On the exact security of Full-Domain-Hash, Lecture notes in computer science, 2000, Vol. 1880:229-235.

[31] Desmedt Y,Quisquater J. Public-key systems based on the difficulty of tampering, Lecture Notes in Computer Science, 1986, Vol. 263:111-117.

[32] *Crescenzo G D, Ostrovsky R, Rajagopalan S. Conditional oblivious transfer and timed-*release encryption, Lecture notes in computer science, 1999, Vol. 1592:74-89.

[33] Dolev D, Dwork C, Naor M. Non-malleable cryptography, SIAM Journal computing, 2000, Vol. 30,No. 2:391-437.

[34] Feige U, Fiat A, Shamir A. Zero-knowledge proofs of identity, Journal cryptology, 1988, Vol. 1:77-94.

[35] Fiat A,Shamir A. How to prove yourself: practical solutions to identification and signature problems, Lecture notes in computer science, 1986, Vol. 263:186-194.

[36] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes, Lecture notes in computer science, 1999, Vol. 1666:537-554.

[37] Frey G, Muller M, Ruck H. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, IEEE Tran. on Info. Th. 1999, Vol. 45:1717-1718.

[38] Galbraith S. Supersingular curves in cryptography, Lecture notes in computer science, 2001, Vol. 2248:495-513.

[39] Galbraith S, Harrison K, Soldera D. Implementing the tate-pairing, Lecture notes in computer science, 2002, Vol. 2369:69-86.

[40] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Robust and efficient sharing of RSA functions,Journal cryptology, 2000, Vol. 13, No. 2:273-300.

[41] Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for

discrete-log based cryptosystems, Lecture notes in computer science, 1999, Vol. 1592: 295-310.

[42] Goldwasser S, Micali S. Probabilistic encryption, Journal computer and system sciences, 1984, Vol. 28:270-299.

[43] Huhnlein D, Jacobson M, Weber D. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders, Lecture notes in computer science, 2000, Vol. 2012:275-287.

[44] Joux A. A one round protocol for tripartite Diffie-Hellman, Lecture notes in computer science, 2000, Vol. 1838:385-394.

[45] Joux A. The weil and tate pairings as building blocks for public key cryptosystems, Lecture notes in computer science, 2002, Vol. 2369:11-18.

[46] Joux A, Nguyen K. Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups, Journal cryptology, 2003, Vol. 16, No. 4:239-247.

[47] Maurer U. Towards proving the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, Lecture notes in computer science, 1994, Vol. 839: 271-281.

[48] Maurer U, Yacobi Y. Non-interactive public-key cryptography, Lecture notes in computer science, 1991, Vol. 547:498-507.

[49] Menezes A, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Tran. on Info. Th. 1993, Vol. 39:1639-1646.

[50] Paillier P, Yung M. Self-escrowed public-key infrastructures, Lecture notes in computer science, 1999, Vol. 1787:257-268.

[51] Tsuji S, Itoh T. An ID-based cryptosystem based on the discrete logarithm problem, IEEE journal on selected areas in communication, 1989, Vol. 7, No. 4:467-473.

[52] Verheul E. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, Lecture notes in computer science, 2001, Vol. 2045:195-210.

[53] Goyal V. Reducing trust in the PKG in identity-based cryptosystems. In: Advances in Cryptology-Crypto 2007, LNCS, 2007, vol. 4622: 430-447.

[54] Xu P, Cui G H, Fu C, et al. A more efficient accountable authority IBE scheme under the DL assumption. Sci china inf sci, 2010, 53: 581-592.

[55] Ren F, Hu L, Zhao K, Liang H, Ren W. ADIC: an anomaly detection algorithm using incremental clustering. Journal of information and computational science, Binary Information Press, 2009, Vol. 6:1051-1057.

[56] Hu L, Ren W, Ren F. Anomaly detection using improved hierarchy clustering. Proceedings of 2009 international conference on artificial intelligence and computational intelligence, Shanghai, 12-15 July, 2009:319-323.

[57] 胡亮,初剑峰,林宇,王首道,金哲. 基于信任服务的 IBE 系统,吉林大学学报(工学版), 2009.5, Vol.39 No.3:137-142.

第八章　基于身份的广播加密算法

8.1　基于身份的广播加密算法介绍

基于身份广播加密(IBBE, identity-based broadcast encryption)的概念由Delerablée在2007年正式提出,不再使用"多接收者的密钥封装机制"的称呼,而称为"基于身份广播加密"来强调这个概念接近于广播加密学和基于身份的加密学。这个概念和基于身份加密相关,也与基于身份的多接收者密钥封装机制相关。在IBBE方案中,一个公开的密钥可以用于加密消息给任意一组身份 S。因此,如果设置 $S=1$,那么IBBE方案就是IBE的方案。一个低效率的实现IBBE的方案是使用IBE来加密消息给每个身份,这样产生的密文个数将随 S 增加而呈现线性增长。因此,也可以把IBBE看做是使广播加密更加有效的方法。

Delerablée提出了IBBE正式的定义以及安全性概念。在定义中,一个IBBE方案包含一个类似于Boneh有关广播加密BE定义中的Extract过程,也可以被认为是一个广义的IBE系统。关于安全性概念,Delerablée延续了BE中的典型安全概念(静态攻击安全),这个安全概念类似于IBE中的选择身份安全(比完全安全弱一些),并提出了关于IBBE的安全性概念及攻击模型,包括IND-sID-CCA和IND-sID-CPA。另外,Delerablée使用一个密钥封装机制KEM构建了一个IBBE方案,该方案使用一个短的对称密钥来加密待广播的长消息。进而,Delerablée证明了其方案达到了静态安全(Delerablée使用IBE中相似的概念,称其为选择身份安全)、选择明文安全(IND-sID-CPA),但是安全性证明要求将密码学哈希函数建模为随机预言机,也就是说,该方案在随机预言机模型下被证明是安全的,而实际应用中不一定安全。在效率方面,Delerablée的方案使用了固定长度的密文和私钥,公钥和接收者数目的最大值呈线性增长,也就是说,该方案达到了 $O(1)$ 大小的密文、$O(n)$ 大小的公钥和固定长度的私钥。由于Delerablée的方案是在随机预言机下证明了选择明文安全,所以该方案在安全性和实用性上有待提高。

在近几年的基于身份广播加密研究进展中,一些新的研究结果也相继出现,如,Guo基于Delerablée的方案提出一个授权的基于身份广播加密方案(A-IBBE, authority identity-based broadcast encryption),该方案提供了一种新方法来

减轻 IBBE 中的密钥托管问题。Guo 在随机预言机下证明了其方案达到了 IND-sID-CPA 安全,但是没有描述方案的效率。将该方案和 Delerablée 的方案的构建相比较,可以认为两者具备相同的效率。在 2008 年,Boneh 和 Hamburg 发现了一种构建 IBE 和 BE 的一般化框架,并且在随机预言机下提出了第一个层次的基于身份广播加密方案(HIBBE,hierarchical identity-based broadcast encryption)。在 Boneh 和 Hamburg 方案中,密文的大小都与相关用户的数目无关,但是私钥大小跟随系统的复杂性而增长。在 2009 年,Gentry 和 Waters 针对 IBBE 提出了等同的"适应性安全"(adaptive security)概念。为了达到适应性安全下的选择密文安全,他们提出了"半静态安全"概念以及由"半静态安全"向"适应性安全"转化的方法。进而,他们提出了第一个适应性安全的 IBBE 方案,具有 $o(\lambda \cdot l)$ 大小的公钥和固定长度的私钥(也就是 $o(\lambda)$)。

本章中的方案都是在基于静态攻击模型下完成安全性证明的,并可以根据 Gentry 和 Waters 的研究结果向更高安全性转化。

8.2 基本定义及基本模型

8.2.1 IBBE 的形式化定义

在有关 IBBE 的安全性讨论中,将使用 Boneh 和 Hamburg 提出的 IBBE 方案的形式化定义,该定义揭示了 IBBE 方案的一般性规律,包括使用混合加密机制来提高效率等,如定义所述:

一个 IBBE 方案包含一个权威中心:私钥产生器 PKG。PKG 通过为每个用户(拥有身份 ID_i)分配私钥 sk_{ID_i},使用户能解密消息。sk_{ID_i} 的产生基于一个主密钥 MSK。

$Setup(\lambda, m)$:输入安全参数 λ 和一次加密中接收者集合的最大数目 m,输出为主密钥 MSK 和公钥 PK。MSK 由 PKG 给出,而 PK 是公共的。

$Extract(MSK, ID_i)$:输入主密钥 MSK 和身份 ID_i,输出身份 ID_i 对应的私钥 sk_{ID_i}。

$Encrypt(S, PK)$:输入公钥 PK 和一个包含用户身份 $S = \{ID_1, \cdots, ID_s\}$(其中 $s < m$)的集合,输出 (Hdr, K),其中 Hdr 叫做报头,$K \in \kappa$,κ 是对称加密方案的密钥集合。

当消息 $m \in \{0,1\}^*$ 将要被广播给 S 中的用户时,广播者生成 $(Hdr, K) \leftarrow Encrypt(S, PK)$,在对称密钥 $K \in \kappa$ 下 m 加密密文 c_m,并且广播 (Hdr, S, c_m)。将 Hdr 作为报头,(Hdr, S) 作为整个报头,K 作为消息加密密钥并且 c_m 作为广播主体。

$Decrypt(S, ID, sk_{ID}, Hdr, PK)$：输入子集 $S = \{ID_1, \cdots, ID_s\}$、身份 ID 和其私钥 sk_{ID}，报头 Hdr 和公钥 PK，如果 $ID \in S$，算法输出消息加密密钥 K，用于解密广播体 c_m 并且恢复消息 m。

注意，在一个 IBBE 系统中，可能的用户数目并不需要在开始时确定，因此不需要讨论全共谋抵抗。如果可能的用户数目确定了，满足该定义的构建就达到了全共谋抵抗。

8.2.2 安全性及攻击模型

BE 的一个标准安全概念是静态攻击下的选择密文安全，而对于 IBE，一个标准概念是选择身份安全，敌手必须在游戏开始前选择一个要攻击的身份。BE 中静态攻击的概念与 IBE 中的选择身份攻击概念相似，区别在于 BE 中敌手选择的是一组要攻击的用户身份，而 IBE 中是一个用户身份。Delerablée 强调采用一个类似于 IBE 中的选择身份安全的较弱的安全模型来定义 IBBE 的安全性，等同于 BE 中的“静态安全”(static security)，我们将 IBBE 中的此类安全定义为静态安全。

IBE 中强的安全概念是完全安全性，即敌手可以适应性地选择要攻击的身份，而不需要提前确定，这样的敌手具备更强的攻击能力。Gentry 和 Waters 针对 IBBE 提出了等同的“适应性安全”(adaptive security)概念，为了达到适应性安全下的选择密文安全，他们提出了“半静态安全”概念以及由“半静态安全”向“适应性安全”转化的方法。

可见，在 IBBE 中有两类安全概念，静态安全和适应性安全，相对应地有两类攻击模型：静态攻击和适应性攻击。在静态攻击模型中，敌手在获得系统的公开参数之前就确定要攻击的一组用户身份，而使得该攻击模型无法覆盖可能的全部攻击类型，比如敌手可能基于公共参数或之前窃取的私钥结构来选择计划窃取的密钥和密文，进而展开攻击，而适应性攻击模型可以覆盖这些情况。因此，适应性安全是 IBBE 更为标准的安全概念。

因为数学复杂性难以通过实验实现，安全性都是通过一个敌手 $\mathcal{A}$ 和一个挑战者的游戏模型来定义。下面分别针对 IBBE 中的静态安全和适应性安全，描述其相应的攻击模型。

首先以算法的形式给出关于密钥查询和解密查询的基础定义，以便于描述敌手对于 IBBE 方案的攻击。

定义 8.1 私钥抽取查询 Et：算法 Et 的输入为一个待查询的身份 ID，执行算法 Et 输出对应于该 ID 的私钥 SK，即 $SK \leftarrow Et(ID)$。

定义 8.2 解密查询 Dt：算法 Dt 输入为一个三元组 (ID_i, S, Hdr)，其中 $ID_i \in S$，挑战者使用 $Decrypt(S, ID, sk_{ID_i}, Hdr, PK)$ 作出响应。

在下面的攻击模型中，敌手 $\mathcal{A}$ 和挑战者都以接收者 S 的最大数量 m 作为输入。通过阻止敌手发布解密查询可以为一个 IBBE 安全方案定义语义安全。

1. 静态攻击模型

静态攻击模型类似于 IBE 中的选择身份攻击模型，敌手首先确定一组要攻击的身份，然后通过发布一系列的私钥抽取查询，来获得某个不在攻击身份集合中的身份对应的私钥，并可能针对该身份进行解密查询（如果是选择明文安全，解密查询将被阻止），通过这些查询为下一步攻击做必要的准备。然后，挑战者随机选择一个 K_0 或 K_1，表示为 K_b，其中 $b \in \{0,1\}$，挑战者对 K_b 加密后将密文返回给敌手，此时敌手可以做出推测或者再次执行查询后做出推测，得出对于 b 的推测值，进而完成一次攻击。

静态攻击模型的描述如下：

初始化：敌手 $\mathcal{A}$ 首先输出一组想要攻击的身份标识 $S^* = \{ID_1^*, \cdots, ID_s^*\}$。

建立：挑战者启动 $Setup(\lambda, m)$ 来获得公钥 PK，然后将公钥 PK 发送给 $\mathcal{A}$。

阶段 1：敌手 $\mathcal{A}$ 自适应地发出查询 $q_1, \cdots, q_t$，其中 q_t 是以下情况之一：

（1）发布有关身份 ID_i（$ID_i \notin S^*$）的抽取查询 Et，并且从挑战者处获得对应的私钥。

（2）发布有关（ID_i, S, Hdr）的解密查询 Dt，接收响应：$Decrypt(S, ID, sk_{ID_i}, Hdr, PK)$。

挑战：当 $\mathcal{A}$ 决定阶段 1 结束时，挑战者执行 $Encrypt$ 算法获得 $(Hdr^*, K) = Encrypt(S^*, PK)$，其中 $K \in \kappa$。然后挑战者随机选择 $b \leftarrow \{0,1\}$，使 $K_b = K$，并且将 K_{1-b} 设置为 κ 中的一个随机值，然后将 (Hdr^*, K_0, K_1) 返回给敌手 $\mathcal{A}$。

阶段 2：敌手再次执行查询后做出推测，过程同阶段 1 和挑战。

猜测：最后，敌手 $\mathcal{A}$ 输出一个猜测 $b' \in \{0,1\}$，如果 $b = b'$，则敌手 $\mathcal{A}$ 获胜。

定义敌手在游戏中可能发布的解密查询的全部数量为 q_D、抽取查询的全部数量为 t。t, m, q_D 作为攻击参数，使用 $Adv_{IBBE}^{ind}(t, m, q_D, \mathcal{A})$ 定义 $\mathcal{A}$ 在游戏中的优势：

$$Adv_{IBBE}^{ind}(t, m, q_D, \mathcal{A}) = \left| Pr[b = b'] - \frac{1}{2} \right|$$

$$= |Pr[b = b' \mid b = 1] - Pr[b' = 1 \mid b = 0]|$$

定义 8.3　静态安全：在上述攻击模型中，一个 IBBE 方案是静态安全的，如果 $\mathcal{A}$ 在所有时间 $poly(\lambda)$ 下，$Adv_{IBBE}^{ind}(t, m, q_D) = negl(\lambda)$。

2. 适应性攻击模型

适应性攻击模型与静态攻击模型不同的是，敌手不会首先确定要攻击的身份集合，而是执行查询后根据查询的结果适应性地确定要攻击的身份集合。适应性攻击模型的描述如下：

建立:挑战者启动 $Setup(\lambda, m)$ 来获得公钥 PK,然后将公钥 PK 发送给 $\mathcal{A}$。

阶段 1:敌手 $\mathcal{A}$ 自适应地发出查询 $q_1, \cdots, q_t$,其中 q_i 是以下情况之一:

(1) 发布有关身份 ID_i 的抽取查询 Et,并且从挑战者处获得对应的私钥。

(2) 发布有关 (ID_i, S, Hdr) 的解密查询 Dt,接收响应:$Decrypt(S, ID, sk_{ID}, Hdr, PK)$。

挑战:当 $\mathcal{A}$ 决定阶段 1 结束时,$\mathcal{A}$ 选择一组想要攻击的身份标识 $S^* = \{ID_1^*, \cdots, ID_s^*\}$,注意,在阶段 1 中执行抽取查询的身份 ID_i 不在要攻击的身份集合 S^* 中,也就是 $ID_i \notin S^*$。挑战者执行 $Encrypt$ 算法来获得 $(Hdr^*, K) = Encrypt(S^*, PK)$,其中 $K \in \kappa$。然后挑战者随机选择 $b \leftarrow \{0,1\}$,集合 $K_b = K$,并且将 K_{1-b} 设置为 κ 中的一个随机值,挑战者将 (Hdr^*, K_0, K_1) 返回给敌手 $\mathcal{A}$。

猜测:最后,敌手 $\mathcal{A}$ 输出一个猜测 $b' \in \{0,1\}$,如果 $b = b'$,则敌手 $\mathcal{A}$ 获胜。

使用 $Adv_{IBBE}^{ind}(t, m, q_D, \mathcal{A})$ 定义 $\mathcal{A}$ 在游戏中的优势:

$$Adv_{IBBE}^{ind}(t, m, q_D, \mathcal{A}) = \left| Pr[b = b'] - \frac{1}{2} \right|$$

$$= |Pr[b = b' | b = 1] - Pr[b' = 1 | b = 0]|$$

定义 8.4 适应性安全:在上述攻击模型中,一个 IBBE 方案是适应性安全的,如果 $\mathcal{A}$ 在所有时间 $poly(\lambda)$ 下,$Adv_{IBBE}^{ind}(t, m, q_D) = negl(\lambda)$。

8.3 预备知识

8.3.1 一般的 DH 指数假设

在第一章 DH 相关问题中介绍了许多 GDH 问题,在本节采用的是 Boneh 和 Hamburg 的一般化 DH 假设(GDHE,general Diffie-Hellman exponent assumption)。

设 $B = (p, G_1, G_2, G_T, e(\cdot, \cdot))$ 为一个双线性映射组系统,$G_1 = G_2 = G$。设 $g_0 \in G$ 为一个 G 的生成元,且 $g = e(g_0, g_0) \in G_T$。设 s, n 为正整数并且 $P, Q \in F_p[X_1, \cdots, X_n]^s$ 为两个 s 元 n 个变量的 F_p 多项式。因此,P 和 Q 为两个包含 s 维多项式的列表。将 P 和 Q 表示为 $P = (p_1, p_2, \cdots, p_s)$ 和 $Q = (q_1, q_2, \cdots, q_s)$,并且 $p_1 = q_1 = 1$。对于任何函数 $h: F_p \rightarrow \Omega$ 和向量 $(x_1, \cdots, x_n) \in F_p$,$h(P(x_1, \cdots, x_n))$ 代表 $(h(p_1(x_1, \cdots, x_n)), \cdots, h(p_s(x_1, \cdots, x_n))) \in \Omega^s$。设 $f \in F_p[X_1, \cdots, X_n]$。说明 f 依赖于 (P, Q),用 $f \in \langle P, Q \rangle$ 来表示,这其中存在一个线性分解:

$$f = \sum_{1 \leqslant i,j \leqslant s} a_{i,j} \cdot p_i \cdot p_j + \sum_{1 \leqslant i \leqslant s} b_i \cdot q_i, a_{i,j}, b_i \in Z_p$$

设 P 和 Q 表示如上,且 $f \in F_p[X_1, \cdots, X_n]$,$(P, Q, f)$ 的一般 Diffie-Hellman 指数问题的定义如下文所述。

定义 8.5　((*P*,*Q*,*f*)-GDHE),给定 $H(x_1,\cdots,x_n)=(g_0^{p(x_1,\cdots,x_n)},g_0^{Q(x_1,\cdots,x_n)})\in G^s\times G_T^s$ 计算 $g^{f(x_1,\cdots,x_n)}$。

定义 8.6　((*P*,*Q*,*f*)-GDDHE),给定 $H(x_1,\cdots,x_n)\in G^s\times G_T^s$ 的表示如上,且 $T\in G_T$,决定是否 $T=g^{f(x_1,\cdots,x_n)}$ 成立。

当 $f\notin\langle P,Q\rangle$ 时,(*P*,*Q*,*f*)-GDHE 和(*P*,*Q*,*f*)-GDDHE 具有相同的安全性。本文给出假设对于任何的 $f\notin\langle P,Q\rangle$ 和多项式参数 $s,n=poly(\lambda)$ 都是难处理的,证明本文的构造在这种假设下是安全的。

8.3.2　两种构建 CCA 安全 IBBE 方案的一般方法

Boneh 和 Hamburg 提出了一个使用固定长度密文和私钥的 IBBE 方案,并且使用 GDDHE 框架证明了 IND-sID-CPA 安全性。在第一章安全性之间的转化与构建方法一节介绍了构建 CCA 安全的方案的方法,本节将提出两种 CCA 安全的 IBBE 系统的构建方法和形式化描述,应用此方法可以将之前的 IBBE 系统转为 CCA 安全的改进方案。

1. 应用一次签名机制

下面的 *IBBE* = (*Setup*,*Extract*,*Encrypt*,*Decrypt*) 是一种新的方案,在方案中使用强一次签名 *Sig* = (∂,*Sign*,*Vrfy*),使得该方案达到了选择密文安全。

Setup:首先运行 *Setup*(λ,*n*)来获得(*PK*,*MSK*),公钥是 *PK*,主密钥是 *MSK*。

Extract:给定 *MSK* 和身份 *ID*,输出 sk_{ID}。

Encrypt:为了使用公钥 *PK* 来加密一个消息 *m*,广播者首先运行∂(λ)来获得验证密钥 V_{SIG} 和签名密钥 K_{SIG}($|V_{SIG}|=l$)。然后广播者使用验证密钥 V_{SIG} 加密消息 *m*。让 $S=\{ID_i\}_{i=1}^{s}$ 为一组目标身份。广播者运行 $Encrypt_{(S,PK)}(V_{SIG})$ 得到 *c*,并运行 $Sign(c,K_{SIG})$ 得到 σ。最终的密文为 (c,σ,V_{SIG})。

Decrypt:对一个身份 $ID_j\in S=\{ID_i\}_{i=1}^{s}$,为了使用主密钥 *MSK* 解密密文 (c,σ,V_{SIG}),接收者首先验证是否 $Vrfy_{V_{SIG}}(c,\sigma)=1$,如果不是,输出"⊥",否则接收者从 *c* 中获得 *m*。

2. 应用 MAC 机制

本节在这里说明一下如何使用消息验证代码和一个"封装方案"取代一次签名机制来达到预期的目的。

设(*Init*,*S*,*R*)为一个安全封装方案,通过长度为 *n* 的身份集合 *S* 输出 *com*,设(*Mac*,*Vrfy*)为一个消息验证代码。接下来的 *IBBE* = (*Setup*,*Extract*,*Encrypt*,*Decrypt*)是一个新的达到抗密文攻击的 *IBBE* 的构建。

Setup:首先运行 *Setup*(λ,*n*)来获得(*PK*,*MSK*),并且运行 *Init*(λ,*n*)生成 *pub*。公钥是(*PK*,*pub*),主密钥是 *MSK*。

Extract:给定 MSK 和身份 ID,输出 sk_{ID}。

Encrypt:为了使用公钥(PK,pub)来加密一个消息 m,广播者首先通过运行 $S(\lambda,pub)$封装一个随机值来得到(r,com,dec)。然后广播者使用 dec 处理消息 m 来得到 $dec\circ m$,并且加密关于 com 的 $dec\circ m$。也就是,广播者通过 $Encrypt_{(S,pk)}(com,dec\circ m)$得到密文 c,那么密文 c 就会被校验,通过使用 r 作为一个消息验证代码的密钥;也就是,广播者计算 $tag=Mac_r(c)$。最终的密文为$\langle com,c,tag\rangle$。

Decrypt:为了解密密文$\langle com,c,tag\rangle$,接收者使用密钥 sk_{ID}来得到 $dec\circ m$(如果解密失败,接收者输出"$\perp$")。接下来,接收者运行 $R(pub,com,dec)$来得到一个字符串 γ;如果 $\gamma\neq$"$\perp$"并且 $Vrfy_\gamma(c,tag)=1$,接收者输出 m,否则输出"$\perp$"。

8.4 基于一次签名的构建

8.4.1 方案描述

在本节将介绍一个采用强一次签名方案的 IBBE 方案,该方案具备固定长度的密文和私钥的特性。

Setup(λ,n):给定一个安全参数 λ 和整数 n,双线性映射组 $B=(p,G_1,G_2,G_T,e(\cdot,\cdot))$被构建如 $|p|=\lambda$。并且,两个生成元 $g\in G_1$、$h\in G_2$ 以及一个秘密值 $r\in Z_p^*$ 都是随机选择的。选择两个密码学哈希函数 $H_1:\{0,1\}^*\rightarrow Z_p$,$H_2:\{0,1\}^l\rightarrow Z_p$。安全分析将把 H_1,H_2 看作随机 Oracle 模型。B 和 H_1,H_2 组成了系统的公用参数。主密钥被定义为 $MSK=(g,r)$,公钥是 $PK=(w,v,h,h^r,\cdots,h^{r^n})$,其中 $w=g^r$,$v=e(g,h)$。

Extract(MSK,ID):给定 $MSK=(g,r)$和身份 ID,输出

$$sk_{ID}=g^{\frac{1}{r+H_1(ID)}}$$

Encrypt(S,PK):广播者首先运行 $\partial(\lambda)$来获得验证密钥 V_{SIG}和签名密钥 K_{SIG}($|V_{SIG}|=l$),假定 $S=\{ID_j\}_{j=1}^s$,$s\leqslant n$。给定 $PK=(w,v,h,h^r,\cdots,h^{r^n})$,广播者随机地选择 $k\leftarrow Z_p^*$ 并且计算 Hdr 和 K:

$$c=(C_1,C_2)=(w^{-k},h^{k\cdot H_2(V_{SIG})\cdot\prod_{i=1}^{S}(r+H_1(ID_i))})$$

$$Hdr=(c,Sign(c,K_{SIG}),V_{SIG})$$

$$K=v^k$$

加密过程输出(Hdr,K),然后 K 被用于加密消息。

Decrypt$(S,ID_i,sk_{ID_i},Hdr,PK)$:从头信息 $Hdr=(c,\sigma,V_{SIG})$重新得到被封装的加密消息的对称密钥 K。

(1) 验证 σ 是否是密钥 V_{SIG} 下有效的 (C_1, C_2) 签名。如果无效，输出“⊥”。

(2) 否则，选择一个随机的 $\beta \in Z_p$ 并且计算：

$$P_1 = \frac{H_2(V_{SIG})}{\gamma}\left(\prod_{j=1,j\neq i}^{s}(\gamma + H_1(ID_j)) - \prod_{j=1,j\neq i}^{s}(H_1(ID_j)) + \frac{\beta}{\gamma}\right)$$

并且

$$P_2 = sk_{ID_i} \cdot g^{\frac{\beta}{\gamma \cdot H_2(V_{SIG}) \cdot \prod_{j=1}^{s}(\gamma + H_1(ID_j))}}$$

(3) 输出

$$K = (e(C_1, h^{P_1}) \cdot e(P_2, C_2))^{\frac{1}{H_2(V_{SIG}) \cdot \prod_{j=1,j\neq i}^{s} H_1(ID_j)}}$$

8.4.2　安全分析

定理 8.1　对于任意的正整数 n，在 GDDHE 假设成立即 $(Adv\sigma^{gddhe}(f,g,F,\mathcal{A}) \leqslant \varepsilon_1)$ 和强签名系统是 (t,ε_2,l) 强存在不可伪造的前提下，以上 IBBE 方案是 $(t,\varepsilon_1+\varepsilon_2,n,q_D)$ CCA 安全的。

证明：假定存在一个 t 时间的攻击者 $\mathcal{A}$，则 $AdvBr_{\mathcal{A},n} > \varepsilon_1 + \varepsilon_2$。建立一种规则 R，在解决 GDDHE 问题中拥有特性 ε_1。规则 R 区分 (f,g,F)-GDDHE 的两种分布。

敌手和挑战者都给定输入用户集合 S 的最大数目 n，敌手可能发布的抽取查询和随机预言机查询数目为 t。运算规则 R 给定一组输入 $B = (p, G_1, G_2, G_T, e(\cdot,\cdot))$，以及一个在 B 中的 (f,g,F)-GDDHE 实例。因此有 f 和 g 两个具有一对不同根的互质的多项式，各自的顺序为 t 和 n，并且 R 给定如下：

$$g_0, g_0^r, \cdots, g_0^{r^{t-1}}, g_0^{r\cdot f(r)}, g_0^{k\cdot r\cdot f(r)}, h_0, h_0^r, \cdots, h_0^{r^n}, h_0^{k\cdot g(r)}$$

$t \in G_T$ 等价于 $e(g_0,h_0)^{k\cdot f(\gamma)}$ 或一些 G_T 中的随机元素。

为了简便，认为 f 和 g 为单多项式，但这并不是强制要求。

定义符号：

$$f(X) = \prod_{i=1}^{t}(X + x_i), \quad g(X) = \prod_{i=t+1}^{t+n}(X + x_i)$$

$$f_i(x) = \frac{f(x)}{x + x_i}, i \in [1,t], \text{是一个深度为 } t-1 \text{ 的多项式}$$

$$g_i(x) = \frac{g(x)}{x + x_i}, i \in [t+1, t+n], \text{是一个深度为 } n-1 \text{ 的多项式}$$

初始化：规则 R 执行 $\mathcal{A}$ 并且得到 $\mathcal{A}$ 想要攻击的身份集合 $S^* = \{ID_1^*, \cdots, ID_{s^*}^*\}(s^* \leqslant n)$。

建立：为了生成系统参数、R 的集合 $g = g_0^{f(\gamma)}$ 和集合

$$h = h_0 \prod_{i=t+s^*+1}^{t+n}(\gamma + x_i), \quad w = g_0^{\gamma\cdot f(\gamma)} = g^{\gamma}$$

$$v = e(g_0, h_0)^{f(\gamma)\cdot\prod_{i=t+s^*+1}^{t+n}(\gamma+x_i)} = e(g,h)$$

R 定义了公钥 $PK=(w,v,h,h',\cdots,h^{r_n})$。在系统参数 g 上执行 $\mathcal{A}$，使用两个 Hash 函数 H_1, H_2（H_1, H_2 为随机预言），具体描述如下：

Hash 查询：在任何时候敌手 $\mathcal{A}$ 可以查询身份 ID_i 上的随机预言机。为了响应这些查询，R 维护了一个三元组 (ID_i, x_i, sk_{ID_i})：

$$\{(*, x_i, *)\}_{i=1}^{t}, \{(ID_i, x_i, *)\}_{i=t+1}^{t+s^*}(*\text{代表一个空实体})$$

当敌手发出一个身份 ID_i 的哈希查询时，

（1）如果 ID_i 已经在列表 L_H 中存在，R 使用相应的 x_i 响应。

（2）否则，R 设置 $H(ID_i)=x_i$，并且使用 $(ID_i, x_i, *)$ 完成列表。

阶段 1：

私钥查询：敌手 $\mathcal{A}$ 发布查询 $q_1,\cdots,q_m$，其中 q_i 是一个抽取查询 (ID_i)：挑战者在 $ID_i \notin S^*$ 上执行抽取，并且将私钥发给敌手。为了生成：

（1）如果 $\mathcal{A}$ 已经发布了 ID_i 上的抽取查询，R 使用列表 L_H 中的 sk_{ID_i} 响应。

（2）否则，如果 $\mathcal{A}$ 已经发布了一个 ID_i 的哈希查询，那么 R 使用相应的 x_i 来计算

$$sk_{ID_i} = g_0^{f_i(\gamma)} = g^{\frac{1}{\gamma+H(ID_i)}}$$

可以证明 sk_{ID_i} 是一个有效的私钥。然后 R 为 ID_i 完成了列表 L_{H_1}。

否则，R 设置 $H(ID_i)=x_i$，计算相应的 sk_{ID_i}，然后为 ID_i 完成了列表 L_{H_1}。

解密查询：规则 $\mathcal{A}$ 发布解密查询，让 (ID_i, S, Hdr) 为一个解密查询，其中 $S \subseteq S^*, ID_i \in S$。让 $Hdr=(C_1, C_2)$，则

（1）使用验证密钥 V_{SIG} 检验在 (C_1, C_2) 中签名 σ。如果签名无效，R 响应“$\perp$”。

（2）如果 $V_{SIG}=V_{SIG}^*$，规则 R 随机选择位 $b \leftarrow \{0,1\}$ 并且终止模拟。

（3）否则，挑战者选择一个随机的 $w \in Z_p$，设置

$$P_1 = \frac{H_2(V_{SIG})}{\gamma}\left(\prod_{j=1,j\neq i}^{s}(\gamma + H_1(ID_j)) - \prod_{j=1,j\neq i}^{s}(H_1(ID_j)) + \frac{\beta}{\gamma}\right)$$

并且

$$P_2 = sk_{ID_i}\cdot g^{\frac{\beta}{\gamma\cdot H_2(V_{SIG})\cdot\prod_{j=1}^{s}(\gamma+H_1(ID_j))}}$$

（4）R 响应 $K = (e(C_1, h^{P_1})\cdot e(P_2, C_2))^{\frac{1}{H_2(V_{SIG})\cdot\prod_{j=1,j\neq i}^{s}H_1(ID_j)}}$。

挑战：当 $\mathcal{A}$ 决定查询阶段 1 结束，R 执行加密来获得：

$$C_1 = g_0^{-k\cdot\gamma\cdot f(\gamma)}, \quad C_2 = h_0^{k\cdot H_2(V_{SIG})\cdot g(\gamma)}, \quad K = T$$

可以验证：

$$C_1 = w^{-k}$$

注意到如果

$$T = e(g_0, h_0)^{k \cdot f(\gamma)}$$

那么

$$K = v^k$$

然后挑战者随机地选择 $b \leftarrow \{0,1\}$，设置 $K_b = K$ 并且设置 K_{1-b} 为一个随机值，返回 (Hdr, K_0, K_1) 给 $\mathcal{A}$。

阶段 2：

私钥查询：敌手 $\mathcal{A}$ 以阶段 1 中相同的方式继续发布查询 $q_{m+1}, \cdots, q_E$，规则 R 继续以阶段 1 中相同的方式响应。

解密查询：规则 R 以阶段 1 中相同的方式响应解密查询。

猜测：最终，敌手 $\mathcal{A}$ 输出一个猜测 $b' \in \{0,1\}$，并且如果 $b = b'$ 规则 R 输出 0（预示着 $T = v^k$。否则，输出 1（预示着 T 是 $G_T g$ 中的一个任意值））。

如果 (g, f, F, R) 是 R_{GDDHE} 的一个样本，那么 $Pr[R(g_0, h_0, \boldsymbol{y}, T) = 0] = \frac{1}{2}$。现在，让“*abort*”作为 R 在模拟过程中终止的事件。那么，当 $(g_0, h_0, \boldsymbol{y}, T)$ 是 P_{GDDHE} 的一个样本时，有：

$$\left| Pr[R(g_0, h_0, \boldsymbol{y}, T) = 0] - \frac{1}{2} \right| \geqslant AdvBr_{\mathcal{A},n} - Pr[abort] > \varepsilon_1 + \varepsilon_2 - Pr[abort]$$

第一个不等式是从实际情况得来的，因此当 $(g_0, h_0, \boldsymbol{y}, T)$ 是 P_{GDDHE} 的一个样本的时候。这个模拟是完美的，R 在解决 GDDHE 时至少拥有优势 $\varepsilon_1 + \varepsilon_2 - Pr[abort]$。

为了完成定理的证明，对于 R 在模拟过程中终止这一事件（$\mathcal{A}$ 的解密查询的一种结果），必须给出这一事件发生的概率的边界值。本文断言 $Pr[abort] < \varepsilon_2$。否则，能利用 $\mathcal{A}$ 伪造签名，而且其概率至少是 ε_2。简而言之，可以构造另外一个知道私钥的挑战者 r，但是收到 K^*_{SIG} 作为已经存在的伪造游戏的一个挑战。在以上的实验中，一个引起终止的原因是发出一个查询，其中包括一个对于某个密文在 K^*_{SIG} 的伪造。挑战者可以用这个伪造来赢得这个存在的伪造游戏。注意，在整个游戏过程中敌手仅仅发出一次选择消息查询，用来产生密文所需要的签名。因此，$Pr[abort] < \varepsilon_2$。

所以，R 的挑战的优势正是所要求的 ε_1。这就完成了定理的证明。

8.5　基于 MAC 方式的构建

通过使用消息验证代码方法来取代一次签名，构建另一种 IBBE 方案，该方案是可证明选择密文安全的。

让(Mac,$Vrfy$)表示 CBC-MAC,使用 λ 位 AES 分组密码体制。

$Setup(\lambda,n)$:给定安全参数 λ 和整数 n,一个双线性映射组 $B=(p,G_1,G_2,G_T,e(\cdot,\cdot))$被构建如 $|p|=\lambda$。并且,两个生成元 $g\in G_1$、$h\in G_2$ 以及一个秘密值 $r\in Z_p^*$ 都是随机选择的。选择一个密码学 Hash 函数 $H_1:\{0,1\}^*\rightarrow Z_p$,$H_2:\{0,1\}^{\lambda_1}\rightarrow Z_p$,$H_3:\{0,1\}^{\lambda_1}\rightarrow Z_p$。$B$ 和 H_1,H_2,H_3 组成了系统的公用参数。主密钥被定义为 $MSK=(g,\gamma)$。

首先,让 $PK=(w,v,h,h^r,\cdots,h^{r^n})$,其中 $w=g^r$,$v=e(g,h)$。然后运行 $Init(\lambda)$来产生 $pub=(h^*,H^*)$,其中 h^* 是一组两两独立的映射 k_1 位字符串到 k 位字符串的 Hash 函数中的一个,H^* 是从普遍一次哈希(UOWHF,universal one-way Hash function)族随机选取的一个$\{H:\{0,1\}^{\lambda_1}\rightarrow\{0,1\}^{\lambda}\}$(其中 $\lambda_1\geqslant 3\lambda$,是安全参数 λ 的一个函数)函数。因此公钥是(PK,pub)。

$Extract(MSK,ID)$:给定 $MSK=(g,\gamma)$和身份 ID,输出 $sk_{ID}=g^{\frac{1}{\gamma+H_1(ID)}}$。

$Encrypt(S,PK,pub)$:

(1) 发送者首先运行封装规则,选择一个随机的 $x\in\{0,1\}^{\lambda_1}$,然后设置 $\gamma=h^*(x)$,$com=H^*(x)$,$dec=x$。

(2) 假定 $S=\{ID_j\}_{j=1}^{s}$,$s\leqslant n$。给定 $PK=(w,v,h,h^r,\cdots,h^{r^n})$,广播者随机地选择 $k\leftarrow Z_p^*$ 并且计算 c(Hdr 的一部分):

$$c=(C_1,C_2)=(w^{-H_2(x)\cdot k},h^{k\cdot H_3(com)\cdot\prod_{i=1}^{S}(\gamma+H_1(ID_i))})$$

并且

$$K=v^{H_2(x)\cdot k}(\text{用于加密消息})$$

注意到 c 封装了加密密钥 K。

(3) 使用密钥 γ 计算在 c 上的一个 MAC:

$$MAC_\gamma(c)=\text{tag}$$

全部密文如下:

$$Hdr=(c,tom,tag)$$

加密输出(Hdr,K)。

$Decrypt(S,ID_i,sk_{ID_i},Hdr,(PK,pub))$:

(1) 首先选择一个随机的 $\beta\in Z_p$ 并且从 c 中恢复 K,也就是计算:

$$P_1=\frac{H_3(com)}{\gamma}\left(\prod_{j=1,j\neq i}^{s}(\gamma+H_1(ID_j))-\prod_{j=1,j\neq i}^{s}(H_1(ID_j))+\frac{\beta}{\gamma}\right)$$

并且

$$P_2=\text{sk}_{ID_i}^{H_2(dec)}\cdot g^{\frac{\beta}{\gamma\cdot H_3(com)\cdot\prod_{j=1}^{s}(\gamma+H_1(ID_j))}}$$

输出

$$K = (e(C_1, h^{P_1}) \cdot e(P_2, C_2))^{\frac{1}{H_3(com) \cdot \prod_{j=1, j\neq i}^{s} H_1(ID_j)}}$$

(2) 计算 $\gamma = H^*(dec)$。

(3) 如果 $Vrfy_\gamma(c, tag) = 1$ 并且 $H^*(dec) = com$，可以使用密钥 K 来恢复得到消息，否则，输出“$\perp$”。

上面使用 *MAC* 的构建比较复杂。这里有三种情况可以将上述方案简单化：

情况 1：

$$c = (C_1, C_2) = (w^{-k}, h^{k \cdot H_3(com) \cdot \prod_{i=1}^{S} (\gamma + H_1(ID_i))})$$

$$K = v^k$$

恢复密钥 K：

$$K = (e(C_1, h^{P_1}) \cdot e(P_2, C_2))^{\frac{1}{H_3(com) \cdot \prod_{j=1, j\neq i}^{s} H_1(ID_j)}}$$

$$P_1 = \frac{H_3(com)}{\gamma}\left(\prod_{j=1, j\neq i}^{s} (\gamma + H_1(ID_j)) - \prod_{j=1, j\neq i}^{s} (H_1(ID_j))\right)$$

情况 2：

$$c = (C_1, C_2) = (w^{-k}, h^{k \cdot H_3(com) \cdot \prod_{i=1}^{S} (\gamma + H_1(ID_i))})$$

$$K = v^k$$

选择一个随机的 $\beta \in Z_p$ 并且从 c 中恢复 K：

$$K = (e(C_1, h^{P_1}) \cdot e(P_2, C_2))^{\frac{1}{H_3(com) \cdot \prod_{j=1, j\neq i}^{s} H_1(ID_j)}}$$

$$P_1 = \frac{H_3(com)}{\gamma}\left(\prod_{j=1, j\neq i}^{s} (\gamma + H_1(ID_j)) - \prod_{j=1, j\neq i}^{s} (H_1(ID_j)) + \frac{\beta}{\gamma}\right)$$

并且

$$P_2 = sk_{ID_i} \cdot g^{\frac{\beta}{\gamma \cdot H_3(com) \cdot \prod_{j=1}^{s} (\gamma + H_1(ID_j))}}$$

情况 3：

$$c = (C_1, C_2) = (w^{-H_2(x) \cdot k}, h^{k \cdot H_3(com) \cdot \prod_{i=1}^{S} (\gamma + H_1(ID_i))})$$

$$K = (e(C_1, h^{P_1}) \cdot e(P_2, C_2))^{\frac{1}{H_3(com) \cdot \prod_{j=1, j\neq i}^{s} H_1(ID_j)}}$$

并且

$$K = v^{H_2(x) \cdot k}$$

$$P_1 = \frac{H_3(com)}{\gamma}\left(\prod_{j=1, j\neq i}^{s} (\gamma + H_1(ID_j)) - \prod_{j=1, j\neq i}^{s} (H_1(ID_j))\right)$$

并且

$$P_2 = sk_{ID_i}^{H_2(dec)}$$

8.6 基于 q-BDHI 的 IBBE 方案

8.6.1 构建方式

本节将基于 q-BDHI 假设提出不使用随机预言机的新的 IBBE 方案，该方案具有固定长度的密文、公钥和私钥。

设 G 是具有素数阶 p 的双线性点群，选择一个抗共谋的密码学 Hash 函数 $H:\{0,1\}^* \rightarrow Z_p^*$，它可以将作为公钥的任意身份字符串映射到 Z_p^* 上。假定用于加密的对称密钥 K 是 G_1 上的一个元素，$K \in \kappa$，κ 是一组对称加密密钥的集合。

Setup(λ, m)：为了产生 IBBE 系统的参数，给定秘密参数 λ 和一个整数 m，同时构建一个双线性映射组系统$(p, G, G_1, e(\cdot,\cdot))$。然后随机选择一个生成元 $g \in G^*$，两个随机元素 $x, y \in Z_p^*$，定义 $X = g^x$，$Y = g^y$。公钥 PK 和主密钥 MSK 定义如下：

$$PK = (g, X, Y), \quad MSK = (x, y)$$

Extract(MSK, ID_i)：现在已知 $MSK = (x, y)$，为了为公钥 $ID_i \in Z_p^*$ 产生相应的私钥：

(1) 选择一个随机元素 $r \in Z_p$，计算 $R = g^{\frac{1}{(r+ID_i)\cdot y + x}}$。

(2) 输出私钥 $sk_{ID_i} = (r, R)$。

在不理想的情况下可能出现 $(r + ID_i) \cdot y + x = 0 (\mathrm{mod}\, p)$，则需要重新选择一个随机元素 r。

Encrypt(PK, N, K)：假定符号 $N = \{ID_j\}_{j=1}^n$ 代表接收者的集合。为了加密对称密钥 $K \in \kappa$，广播者需要随机选择一个秘密值 $s \in Z_p^*$，使用 PK 和 s 来封装对称密钥，计算报头 $Hdr = (A, B, C, D)$，其中：

$$A = Y^{\prod_{j=1}^{n} ID_j \cdot s}, \quad B = X^s, \quad C = Y^s, \quad D = e(g,g)^s \cdot K$$

应该注意到，对于每次加密 $e(g,g)$ 是可以预先计算出来的，因此，加密过程不需要任何对运算。

Decrypt$(PK, N, ID_i, sk_{ID_i}, Hdr)$：为了获得封装在报头 $Hdr = (A, B, C, D)$ 中的对称密钥 K，在集合 $N = \{ID_j\}_{j=1}^n$ 中的接收者（身份 $ID_i \in N (1 \leqslant i \leqslant n)$，私钥 $sk_{ID_i} = (r, R)$）计算和输出 $D / e(A^{1/(\prod_{j=1, j\neq i}^{n} ID_j)} \cdot B \cdot C^r, R)$。事实上，对于有效的密文，有：

$$\frac{D}{e(A^{1/(\prod_{j=1, j\neq i}^{n} ID_j)} \cdot B \cdot C^r, R)} = \frac{D}{e(g^{y \cdot ID_i \cdot s} \cdot g^{(x)\cdot s} \cdot g^{(y)\cdot s \cdot r}, g^{\frac{1}{(r+ID_i)\cdot y + x}})}$$

$$= \frac{e(g,g)^{s} \cdot K}{e(g,g)^{s}} = K$$

8.6.2 安全分析

本节在判定 q-BDHI 假设下，证明上述的不使用随机预言机的 IBBE 方案达到了静态安全概念下的选择明文安全。

定理 8.2 设(t,q,ε)-BDHI 判定假设下，对于点群 G(阶为 $|G|=p$)。如果对于任何的 $q_D < q, t' < t - \theta(\tau q^2)$($\tau$ 是 G 上取幂的最大时间)，之前定义的 IBBE 系统是静态安全概念下的选择明文安全。

证明：接下来的部分将证明定理 8.2。假定敌手 $\mathcal{A}$ 在攻击该 IBBE 系统时具有优势 ε。构建一个算法 $\mathcal{B}$ 使用 $\mathcal{A}$ 来解决 G 上的判定 q-BDHI 问题。算法 $\mathcal{B}$ 给定输入为一个随机的$(q+2)$元素组$(g, g^{a}, g^{a^2}, \cdots, g^{a^q}, T) \in (G^*)^{q+1} \times G_1$。算法 $\mathcal{B}$ 的目标是，如果 $T = e(g,g)^{1/a}$输出 1，否则输出 0。算法 $\mathcal{B}$ 通过与 $\mathcal{A}$ 进行下面的静态安全概念下的选择明文安全游戏进行交互：

准备：算法 $\mathcal{B}$ 构建一个生成元 $h \in G^*$，对于随机的 $w_1, w_2, \cdots, w_{q-2} \in Z_q^*$，$\mathcal{B}$ 知道形如$(w_i, h^{1/(a+w_i)})$的 $q-1$ 对二元组。$\mathcal{B}$ 是如下工作的：

(1) 随机选择 $w_1, w_2, \cdots, w_{q-2} \in Z_q^*$，设 $f(z)$ 为一个多项式，且 $f(z) = \prod_{i=1}^{q-2}(z + w_i)$，展开每一项后得到 $f(z) = \prod_{i=0}^{q-2} c_i z_i$，常数项 c_0 不为 0。

(2) 计算 $h = \prod_{i=1}^{q-1}(g^{(a)^i})^{c_{i-1}} = g^{af(a)}$ 以及 $u = \prod_{i=1}^{q-1}(g^{(a)^{i+1}})^{c_{i-1}} = g^{a^2 f(a)}$。注意其中 $u = h^a$。

(3) 检查 $h \in G^*$。事实上如果 G 上 $h=1$，意味着 $w_j = -a$，w_j 是一些容易识别的身份。在这种情况下，$\mathcal{B}$ 能够直接地解决这次挑战。因此，假定所有的 $w_j \neq -a$。

(4) 观察到对于任意的 $i=1,\cdots,q-2$，$\mathcal{B}$ 很容易构造对$(w_i, h^{1/(a+w_i)})$，有：

$$f_i(z) = \frac{af(z)}{aw_i} = \frac{f(z)}{w_i} = \sum_{j=0}^{q-2} \frac{c_j}{w_i} z^j = \sum_{j=0}^{q-2} d_j z^j$$

那么

$$h^{\frac{1}{aw_i}} = g^{f_i(a)} = \sum_{j=0}^{q-2} (g^{(a^j)})^{d_j}$$

(5) 最后，$\mathcal{B}$ 计算：

$$T_h = T_0^{c_0^2} \cdot T_0$$

其中 $T_0 = \prod_{i=0}^{q-2}\prod_{j=0}^{q-3} e(g^{(a)^i}, g^{(a)^j})^{c_i c_j + 1}$。

注意到当 $T=e(g,g)^{1/a}$ 时，有 $T_h=e(g^{f(a)/a},g^{f(a)})=e(h,h)^{1/a}$。相反，如果 T 在 G_1 上是均匀分布的，那么就是 T_h。

在整个模拟过程中，将使用值 h,u,T_h 和对 $(w_i,h^{1/(a\cdot w_i)})(i=1,\cdots,q-2)$。

初始化：

对于静态攻击游戏，首先敌手输出一个他想要攻击的身份集合 $N=\{ID_j^*\}_{j=1}^n$。

准备：

为了产生系统参数，算法 $\mathcal{B}$ 执行如下操作：

(1) 随机产生 $a,b\in Z_p^*$，且 $b=\prod_{j=1}^{n} ID_j^*$。

(2) 计算 $X=u^{a+b}=h^{a(a+b)}$ 及 $Y=u=h^a$。

(3) 将 $PK=(h,X,Y)$ 作为公开密钥公布。注意到在敌手看来 X,Y 是独立于身份 ID_j^* 的。

(4) 隐式的定义 $x=a(a+b)$ 和 $y=a$，因此 $X=h^x,Y=h^y$，算法 $\mathcal{B}$ 不知道 x 和 y 的值。

阶段 1：

敌手 $\mathcal{A}$ 发布 $q_D<q-1$ 个私钥查询。考虑第 i 次对于身份 $ID_i\notin\{ID_j^*\}_{j=1}^n$ 的私钥抽取查询。算法 $\mathcal{B}$ 以私钥 $(r,h^{\frac{1}{(r+ID_i)\cdot(y+x)}})$ 响应，其中 r 在 Z_p 上均匀分布。响应步骤如下：

(1) 设 $(w_i,h^{1/(a\cdot w_i)})$ 是准备阶段的第 i 次构建的对，定义 $h_i=h^{1/(a\cdot w_i)}$。

(2) $\mathcal{B}$ 首先构造一个 $r\in Z_p$ 满足 $(r+a+b)\cdot aw_i=(r+ID_i)\cdot y+x$。代入 x 和 y 的值后等式便为：

$$(r+a+b)\cdot aw_i=(r+ID_i)\cdot a+a(a+b)$$

可见未知的 a 可以从等式中约掉，并且得到 $\mathcal{B}$ 可以计算出的

$$r=\frac{ID_i}{w_i-1}-(a+b)\in Z_p$$

(3) 现在，$(r,h^{\frac{1}{r+a+b}})$ 是一个身份 ID_i 的有效私钥，因为

$$h_i^{\frac{1}{r+a+b}}=(h^{\frac{1}{aw_i}})^{r+a+b}=h^{\frac{1}{(r+ID_i)\cdot(y+x)}}$$

满足私钥形式的要求。从 r 的构建中可以看出 Z_p 上的所有元素都是均匀分布的，且 $(r+ID_i)\cdot y+x\neq 0, r\neq -(a+b)$。

挑战：

敌手 $\mathcal{A}$ 输出两个消息 $m_0,m_1\in G_1$。算法 $\mathcal{B}$ 选择一随机位 $b\in\{0,1\}$ 和一个随机的 $l\in Z_p^*$，以密文 $ct=(h^{b\cdot l},h^{(a+b)\cdot l},h^l,T_h^l\cdot m_b)$ 响应。定义 $s=l/a$。另一方面，如果 $T_h=e(g,g)^{1/a}$，有：

$$h^{b\cdot l} = h^{\prod_{j=1}^{n} ID_j^* \cdot l} = h^{a\cdot \prod_{j=1}^{n} ID_j^* \cdot s} = Y^{\prod_{j=1}^{n} ID_j^* \cdot s}$$

$$h^{(a+b)\cdot l} = h^{a\cdot(a+b)\cdot s} = (h^x)^s = X^s$$

$$h^l = h^{a\cdot s} = Y^s$$

由上可知，ct 是 ID^* 下有效的 m_b 的加密，其中均匀分布的随机值 $s = l/a \in Z_p^*$。另一方面，当在 G_1 中的 T_h 均匀分布时，在敌手看来，ct 是完全独立于 b 的。

阶段 2：

敌手 $\mathcal{A}$ 发布更多的私钥抽取查询，最大数目满足 $q_D < q - 1$。算法 $\mathcal{B}$ 所做的响应和阶段 1 一样。

猜测：

最后，$\mathcal{A}$ 输出一个猜测值：$b' \in \{0,1\}$。如果 $b = b'$，$\mathcal{B}$ 输出 1，意味着 $T = e(g,g)^{1/a}$，否则，输出 0，意味着 $T \neq e(g,g)^{1/a}$。

当输入元素是从 P_{BDHI}（其中 $T = e(g,g)^{1/a}$）中的抽样时，那么有 $T_h = e(h,h)^{1/a}$。在这种情况下，$\mathcal{A}$ 必须满足 $|Pr[b = b'] - 1/2| > \varepsilon$。另一方面，当输入元组是从 R_{BDHI}（其中 T 在 G_1 上均匀分布），那么有 T_h 在 G_1 上独立均匀分布。在这种情况下，$|Pr[b = b']| = 1/2$。因此，g 在 G^* 中均匀分布、x 在 Z_p^* 中均匀分布和 T 在 G_1 中均匀分布的情况下，有：

$$|Pr[B(g,g^x,\cdots,g^{x^q},e(g,g)^{1/x}) = 0] - Pr[B(g,g^x,\cdots,g^{x^q},T) = 0]|$$

$$\geqslant \left|\left(\frac{1}{2} \pm \varepsilon\right) - \frac{1}{2}\right| \geqslant \varepsilon$$

满足要求。

参 考 文 献

[1] Zhao X, Zhang F. Analysis on Hu et al. 's Identity-based broadcast encryption, International journal of network security, 2011, Vol. 12, No. 3:362-364.

[2] Hu L, Liu Z, Cheng X. Efficient identity-based broadcast encryption without random oracles, Journal of computers, 2010, Vol. 5, No. 3:331-336.

[3] Ramkumar M. Broadcast authentication with preferred verifiers, International journal of network security, 2007, Vol. 4, No. 2:166-178.

[4] Ren Y, Gu D. Fully CCA2 secure identity based broadcast encryption without random oracles, Information processing letters, 2009, Vol. 109, No. 11:527-533.

[5] Mu Y, Susilo W, Lin Y. Identity-based broadcasting, Lecture notes in computer science, 2003, Vol. 2904:177-190.

[6] Anzai J, Matsuzaki N, Matsumoto T. A quick group key distribution scheme with "entity revocation", Lecture Notes in computer science, 2004, Vol. 1716:333-347.

[7] Boneh D, Franklin M. Identity based encryption from the weil pairing, Lecture Notes in

computer science,2001, Vol. 2139:213-229.

[8] Boneh D, Gentry C, Waters B. Collusion-resistant broadcast encryptionwith short ciphertexts and private keys, Lecture notes in computer science, 2005, Vol. 3621:258-275.

[9] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing, Lecture notes in computer science, 2001, Vol. 2248:514-532.

[10] Fiat A, Naor M. Broadcast encryption, Lecture notes in computer science, 1994, Vol. 773:480-491.

[11] Gentry B, Silverberg A. Hierarchical ID-based cryptography, Lecture notes in computer science, 2002, Vol. 2501:548-566.

[12] Joux. A one round protocol for tripartite Diffie-Hellman, Lecture notes in computer science, 2000, Vol. 1838:385-394.

[13] Menezes, Okamoto T, Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field, IEEE transaction on information theory, 1993, Vol. 39:1639-1646.

[14] Mu Y, Varadharajan V. Robust and secure broadcasting, Lecture notes in computer science, 2001, Vol. 2247:223-231.

[15] Naor M,Pinkas B. Efficient trace and revoke schemes, Lecture notes in computer science, 2001, Vol. 1962:1-20.

[16] Verheul E R. Self-blindable credential certificates from the weil pairing, Lecture notes in computer science,2001, Vol. 2248:533-551.

[17] Zhang F, Kim K. ID-based blind signature and ring signature from pairings, Lecture notes in computer science, 2002, Vol. 2501:533-547.

[18] Boneh, D Gentry C, Waters B. Collusion-resistant broadcast encryptionwith short ciphertexts and private keys, Lecture notes in computer science, 2005, Vol. 3621:258-275.

[19] Canetti R, Halevi S,Katz J. A forward-secure public-key encryption scheme, Lecture notes in computer science, 2003, Vol. 2656:255-271.

[20] Canetti R,Halevi S, Katz J. Chosen-ciphertext security from Identity-Based Encryption, Lecture notes in computer science, 2004, Vol. 3027:207-222.

[21] Dodis Y, Yampolskiy A. A verifiable random function with short proofs and keys, Lecture notes in computer science, 2005, Vol. 3386:416-431.

[22] Kurosawa K,Desmedt Y. A new paradigm of hybrid encryption scheme, Lecture notes in computer science, 2004, Vol. 3152:426-442.

[23] Shamir A. Identity-based cryptosystems and signature schemes, Lecture notes in computer science, 1984, Vol. 196:47-53.

[24] Barreto P, Kim H, Lynn B,Scott M. Efficient algorithms for pairing-based cryptosystems, Lecture notes in computer science, 2002, Vol. 2002:354-369.

[25] Bellare M, Boldyreva A, Micali S. Public-key encryption in a multi-user setting: security proofs and improvements, Lecture notes in computer science, 2000, Vol. 1807:259-274.

[26] Desmedt Y, Quisquater J. Public-key systems based on the difficulty of tampering, Lecture notes in computer science, 1986, Vol. 263:111-117.

[27] Frey G, Muller M, Ruck H. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, IEEE Tran. on Info. Th., 1999, Vol. 45:1717-1718.

[28] Gemmell P. An introduction to threshold cryptography, in CryptoBytes, A Technical Newsletterof RSA Laboratories, 1997, Vol. 2, No. 7.

[29] Huhnlein D, Jacobson M, Weber D. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders, Lecture notes in computer science, 2000, Vol. 2012:275-287.

[30] Paillier P, Yung M. Self-escrowed public-key infrastructures, Lecture notes in computer science, 1999, Vol. 1787:257-268.

[31] Gentry C. Practical identity-based encryption without random oracles, Lecture notes in computer science, 2006, Vol. 4004:445-464.

[32] Diffie W, Hellman M E. New directrions in cryptography, IEEE transaction on information theory, 1976, Vol. 22, No. 6:644-654.

[33] Rivest R L, Shamir A, Adelman L. A method for obtaining digital signatures and public-key cryptosystem, Communications of ACM, 1987, Vol. 21, No. 2:120-126.

[34] ElCamal T. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE transaction on information theory, 1985, Vol. 31, No. 4:469-472.

[35] Goldwasser S, Micali S. Probabilistic encryption, Journal of computer and system sciences, 1984, Vol. 28, No. 2:270-299.

[36] Micali S, Rackoff C, Sloan R. The notion of security for probabilistic cryptosystems, SIAM journal on computing, 1988, Vol. 17, No. 2:412-426.

[37] Dolev D, Dwork C, Naor M. Non-malleable cryptography, SIAM journal on computing, 2000, Vol. 30:391-437.

[38] Goldreich O. A uniform complexity treatment of encryption and zero-knowledge, Journal of cryptology, 1993, Vol. 6, No. 1:21-53.

[39] Tsujii S, Itoh T. An ID-based cryptosystem based on the discrete logarithm problem, IEEE journal on selected areas in communication, 1989, Vol. 7, No. 4:467-473.

[40] Maurer U M, Yacobi Y. A non-interactive public-key distribution system, Designs, Codes and cryptography, 1996, Vol. 9, No. 3:305-316.

[41] Hu L, Liu Z, Cheng X, Sun T. A chosen-ciphertext secure identity-based broadcast encryption scheme. Proceedings of the eighth international conference on machine learning and cybernetics, Baoding, 12-15 July, 2009:3556-3560.

[42] Sun T, Hu L, Cheng X, Liu Z. TLS protocol extensions for web applications of identity-based encryption. Proceedings of the eighth international conference on machine learning and cybernetics, Baoding, 12-15 July, 2009:3595-3599.

[43] 胡亮,刘哲理,孙涛,刘芳. 基于身份密码学的安全性研究综述, 计算机研究与发展,

2009.9, Vol.46 No.9:1537-1548.

[44] Hu L, Liu Z, Cheng X. Efficient identity-based broadcast encryption without random oracles. Journal of computers, Mar,2010, Vol 5, No 3:331-336.

第九章　基于身份密码系统的应用

9.1　密钥定时更换机制

之前章节已经介绍了基于身份密码系统的基本思想及方案。本章将介绍利用基于身份密码系统开发的应用实例。在说明具体实例应用之前，首先介绍我们针对在开发过程中遇到的问题，对基于身份密码体制的修改。开发的过程中，我们发现以下一些基于身份密码系统在实际应用中的问题：

（1）椭圆曲线的密码长度越长，则系统的安全性也越高，但是密钥长度越长，加解密和签名等操作的实现时间也越长，同时密钥管理机制根据用户身份计算用户私钥所花费的开销也越大。

（2）随着时间推移，域内的恶意攻击者可能会通过收集用户的公/私钥对来尝试破解系统的主密钥。

（3）某些有特定要求的系统要求所有的数据报能够定时销毁。

为了解决以上问题，在不增加密钥长度的前提下，又要保证体系拥有很高的安全强度，我们采用密钥定时更换机制。

9.1.1　研究内容

针对现有的 IBE 系统存在的问题，我们设计了一个基于信任服务的 IBE 系统。这个系统具有集中式的信任服务，人们可以通过它安全、方便、透明地使用系统所支撑的具体服务。这个系统较好地解决了网络信任保障关键技术的前四个方面内容。

基于信任服务的 IBE 系统由四个部分组成：定时更换的密钥管理机制、统一身份的标识管理机制、集中审计的权限管理机制、域间互连模块的管理机制。这四个机制彼此相互信任，四者之间的关系如图 9.1 所示。

图 9.1 中，标识管理是域内用户进入系统使用服务的入口。请求服务的域内用户首先向标识管理模块发送申请密钥的请求，标识管理机制对该用户进行认证，将通过认证的合法用户的请求报文用数字签名和数字信封进行封装，并发送给密钥管理模块。密钥管理模块只向标识管理模块认证为合法的用户发放私钥。

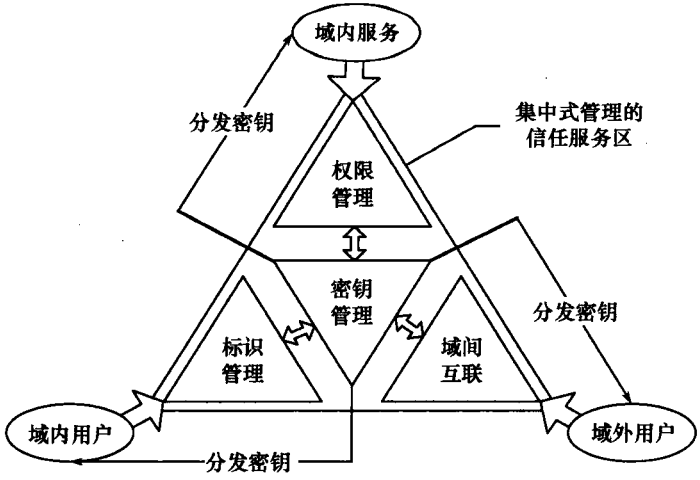

图 9.1 基于信任服务的 IBE 模型

在 IBE 体系下,私钥是集中管理的,即所有私钥都是根据系统的主密钥生成得来。一旦密钥管理机制更换了自己的主密钥,它就更换了域内所有的私钥。具体包括以下内容:

(1) IBE 中主密钥的生成。通过使用随机数生成算法选取一个随机数,然后由其生成系统主密钥。

(2) 用户密钥的生成。当通过验证的用户申请密钥时,根据用户标识能及时为用户生成用户密钥。

(3) 密钥的更新。需要设计一个定时器,定时器触发条件满足时,更换用户的密钥表。

利用密钥更新机制功能,可以使基于身份的密码机制完成以下功能:

(1) 提高系统的安全性,软件主要功能是为用户生成密钥,并定时更换用户密钥表。

(2) 计算 IBE 系统的主密钥。系统启动时,首先为系统生成两个主密钥。

(3) 计算 IBE 系统的系统参数。根据生成的主密钥,计算 IBE 系统的系统参数。

(4) 计算用户私钥。通过 IBE 中标识管理验证的用户向系统申请密钥时,系统根据用户标识计算用户的私钥,并保存。

(5) 更换系统主密钥、系统参数和用户私钥表。系统设置一个定时器,当系统达到定时触发条件时,系统瞬间将密钥表切换为最新密钥表,并继续生成新的主密钥和密钥表。

9.1.2　设计与实现

1. 系统设计

为了实现上述内容，具体实现的架构如图 9.2 所示。

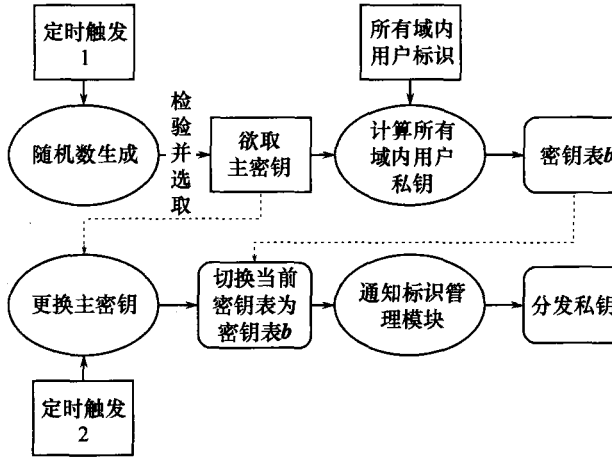

图 9.2　密钥定时更换

2. 系统初始化

根据随机数生成算法任意选取一个随机数，根据这个随机数生成系统主密钥。

根据生成的主密钥，生成系统参数 $Ppub = s \cdot G$。

为了保证密钥的瞬间更换，系统初始时，生成两个主密钥 $s1$，$s2$ 以及对应的系统参数 $Ppub1$ 和 $Ppub2$。

根据生成的主密钥和用户标识计算用户的私钥，生成两张密钥表 a 和 b。

3. 定时触发

向所有机制、所有域内用户发放新的系统参数 $T = (p, a, b, G, Ppub2, q, h, H, I, H1, I1)$。

将事先产生的密钥表 b 作为当前密钥表。

将密钥表 a 存入历史记录表中。

生成新的主密钥和系统参数，产生新的密钥表。

4. 成果与水平

采用随机数生成算法选取随机数生成 IBE 系统主密钥，根据主密钥生成系统参数。已通过标识管理机制验证的用户申请密钥时，可实时为用户生成私钥。达到定时触发条件时，可实现瞬间密钥更换。

9.2 基于密钥定时更换机制的应用

9.2.1 防伪码系统

随着计算机技术的日益发展与普及,有必要在产品防伪,打假方面加强立法。目前,一些不法分子为牟取暴利,专门仿冒名优和畅销产品,以次充好,以假乱真,形成了有一定规模的假冒商品市场,严重扰乱了社会经济秩序,成为阻碍我国经济健康发展的一股浊流。而且,假冒伪劣产品屡禁不止,甚至还有进一步蔓延之势,假冒伪劣产品的数量和范围也呈扩大趋势。从世界范围来说,目前,造假已成为世界各国仅次于贩毒的第二大社会公害,这无疑给广大深受其害的消费者带来了巨大的经济损失和精神伤害。

近年来,由于大量假冒伪劣产品的出现,打击假冒伪劣产品受到了政府和有关部门的高度重视,并采取了一系列措施。我国的防伪技术虽然有很大发展与提高,但与当前市场需要仍有较大差距。目前,世界上包装印刷的假冒制品每年以20%的速度增长,而防伪产品每年却只有8%左右的增长,且技术含量高的防伪技术又较少,所以当前面临的形势仍很严峻,打假、治假任务仍很艰巨。

防伪技术是一门交叉边缘学科,涉及光学、化学、物理学、电磁学、计算机技术、光谱技术、印刷技术、数码印刷技术、包装技术等诸多领域。过去,我国防伪技术的应用仅局限于政府、银行、海关、税务、经济以及社会公共安全等部门制作护照、证件、货币和有价证券等。现在,随着市场经济和商品生产的迅速发展,商标和标识的印制、商品的包装也日趋高档化、精美化和安全化(要求具有防伪功能)。特别是烟酒、饮料、调味品、药品、保健品、化妆品、洗涤用品以及光盘制品等商品的标识和包装越来越多地采用了防伪技术。常用的防伪技术有防伪油墨、防伪纸张、防伪不干胶、微缩文字印刷、票据特种防伪印刷、安全线、加密技术、激光全息转移纸技术、定位烫印、电话电码防伪、原子核双卡防伪核径迹、防伪标识以及手工雕刻凹版印刷等。

目前市场上采用的数码防伪技术几乎全部都是建立数据库,依靠数据检索核对随机组合生成的产品查询号码。当产品数据库的容量达到一定程度时,检索数据量极其庞大,产品的查询效率将受到严重影响。同时这些网络查询通常无法为用户提供鉴别产品真伪的其他辅助手段,如产品特性、使用方法等众多信息。

针对以上问题,我们提出了一种基于身份的商品双重防伪机制可以有效地克服上述缺点。

1. 符号定义

定义 1　流水号 L 是一个根据每个最小销售单元的信息(生产日期、产品编号、产品名称、批次、件号、盒号)生成的一段固定长度的字符串,根据该字符串即可获取对应的产品信息。

定义 2　查询号 C 是一个为用户提供辨别产品真伪的查询编码,它是由流水号经过变换生成的,与流水号一一对应,并且是唯一的,因此可以作为产品的一个身份标识。

定义 3　防伪码 F 是一个为产品提供第二层防伪查询的编码,每个查询号都有与它相对应的一个防伪码。

原理描述如图 9.3 所示。

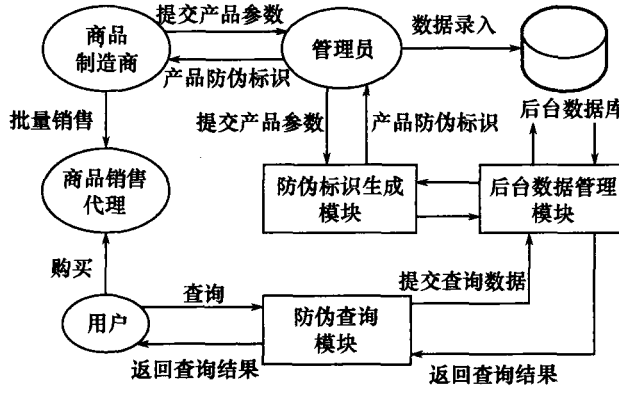

图 9.3　防伪原理图

(1) 商品制造商将要出厂的一批产品参数提交给管理员,获得该批次的所有最小销售单元的防伪标签码(C,F)的列表;由商品制造商负责为每个最小销售单元附上相应的防伪标签。

(2) 管理员负责审核商品制造商提交的产品参数并提交给防伪标识生成模块,获取已生成的防伪标识列表并提交给商品制造商,同时将合法的、已经生成防伪标识的同一批次产品参数,包括生产日期、产品编号、产品名称、总件数、总盒数等录入到后台数据库中,提供合法产品验证。

(3) 防伪标识生成模块根据管理员提交的产品参数:生产日期、批次、产品编号、总件数、总盒数,为每个最小销售单元生成流水号 L 并采用对称加密技术加密流水号 L 生成与流水号 L 一一对应的产品查询号 C。当密钥取定后,对每一个明文分组都有唯一的密文与之对应,因此产品查询号可以作为产品的唯一身份,产品防伪码就是根据该唯一身份生成。

(4) 防伪查询模块负责用户查询数据的管理并提交后台数据管理模块;由

后台数据管理模块处理查询数据并返回查询结果。

2. 具体实现

(1) 初始化:包括对称密钥的生成以及 *Setup* 过程。

(2) 产品编码:即将产品信息编码为如图 9.4 所示的产品流水号。

图 9.4 产品编码

(3) 产品查询号的生成:即 $C = Z_{36}(EK(L))$——首先对产品流水号用系统初始化过程中选取的对称密钥进行加密后,再将得到的密文转换为 36 进制形式。

(4) 产品防伪码的生成:将产品查询号作为一个产品的唯一身份标识,并根据该身份标识生成对应私钥。过程如下:① $Q_{ID} = H_1(C)$;② 生成私钥 $d_{ID} = s^* Q_{ID}$;③ $F = Z_{36}[CRC_{32}(x) \| CRC_{32}(y)]$ 或 $F = Z_{36}[HASH_{64}(x \| y)]$。

(5) 商品验证:过程如图 9.5 所示。

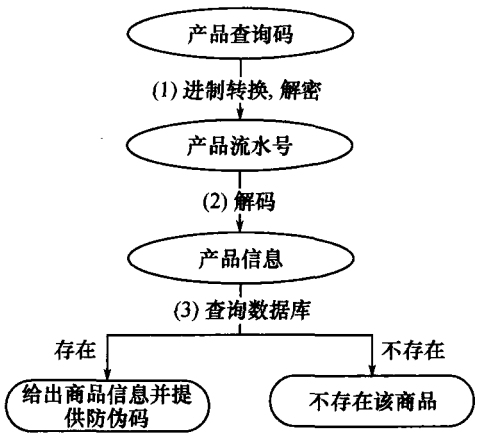

图 9.5 产品验证过程

3. 技术特点

(1) 批量生成:对于一批货物,管理员只需要提交该批货物的特征信息,防伪标识生成模块就会自动为该批货物中的每一个最小销售单元分别编号并生成相应查询号及防伪码。

(2) 海量数据查询:设一批货物中共有 M 件产品,每一件产品中包含 N 盒最小销售单元。在现有的产品防伪技术中,$M * N$ 个单元需要在数据库中保存

$M*N$ 个数据记录，而在该方案中，$M*N$ 个单元对应一条数据库记录，相对于目前已有的方案节省了海量数据查询时间。

（3）双重防伪机制：由于产品查询号本身就可以提供一层产品防伪功能，并且由对称密码算法可以推出，产品查询号是具有唯一性的，这样就不存在两个产品防伪标签 $(C_1,F_1),(C_2,F_2)$，使得 $C_1=C_2$ 且 $F_1=F_2$。防伪码作为一个对查询号的第二重验证标识，即使在生成防伪码时使用了压缩算法，也不会影响用户对产品查询号的防伪验证。

9.2.2　文件加密管理系统

随着技术的发展和进步，计算机网络和移动存储设备已成为企业与企业、人与企业以及人与人沟通的重要工具之一。对于企业而言，无论是通过 Internet 的对外通信，还是通过 Internet 的内部通信，或是通过移动介质的通信，都已经完全离不开网络及相关通信工具的使用。

但是，在网络和移动介质通信方便、高效的背后，却隐藏着安全管理上的巨大漏洞和风险。因为，通过网络和移动介质对外开放的情况下，企业很难有效控制员工将资料外流泄露的行为。尽管采用各种方式进行监控防堵，隐患总是防不胜防。被动的监管总有百密一疏的时候。内部人员其实可轻易透过 Internet 等渠道，采用各种已知或未知的手段，将资料外流出去。如此，对企业所带来的技术上的、经济利益上的以及品牌价值上的损害，将是非常严重的，甚至是致命的。

在商业竞争日益激烈的今天，为了有效保护企业的知识产权和智力产品，从而保持企业的核心竞争力，维护其商业利益和品牌价值，完全有必要事先对存储在员工电脑上的重要文件加密，防止企业内部信息的泄露以及保护企业内部的重要文件。

文件加密管理系统就是在这样的背景下正日益成为数据安全化的一种选择。人们已习惯将各种文档资料保存在计算机中，一系列信息安全问题也变得突出：文件泄露、文件受病毒及恶意代码的攻击、由于误操作文件受损坏等。例如，某党政部门内网中，某秘密级别高的文件只能由高可信用户访问，而低可信用户不能进行任何的文件访问操作。如何将文件的保护与访问控制结合来保护计算机文档的安全成为信息安全的一类热点问题。保护信息最常用的技术是数据加密。根据文件读写流程，可以在不同层次对文件进行加密保护：应用层加密、文件过滤驱动加密、磁盘加密等。虽然它们在实现、性能等方面各有特点，但是也都存在某些不足。如应用层加密严重依赖相关应用程序，文件过滤驱动加密和磁盘加密都不能针对用户权限、文件的安全级别进行区分。

针对这些问题，基于 Windows NT 内核操作系统的文件系统驱动框架提出一个更加完善的文件加密系统的方法：引入基于身份认证管理功能模块结合 AES

算法,实现了对用户访问权限进行认证和管理,对指定文件进行透明加解密,对指定文件按照分级原则进行访问控制的功能。该技术在核心态实现,具备更安全、实时加解密、在细粒度上进行访问控制等特点,适用于 Windows 2000 系统及后续版本下的文件系统格式,且不依赖于具体应用。

本系统对存储于本地的文件进行加密、管理,开发对存储于本地的文件进行加密保护,防止非法用户对加密文件进行非授权地读、写、执行等操作,对于泄密的文件可以对相关人员追究责任。本系统采用基于身份密码系统与对称密码 AES 相结合的方法来实现。利用基于 IBE 的文件加密系统客户端,通过连接服务器取得用户私钥,用私钥解开存放在本地的 AES 对称密钥,用对称密钥加解密文件,以实现文件的安全保护。

1. 主要功能

登录功能:异常处理,安全通信等机制,对用户的访问控制进行管理。

加解密功能:对文档、文件夹可以根据安全需求进行不同等级的加解密,以实现对文件的安全保护。

2. 设计原理

(1) 和服务器进行安全通信

IBE:基于身份的加密技术,利用公钥密码体制,可以实现客户端和服务器端的安全通信,获得用户私钥。如图 9.6 所示。

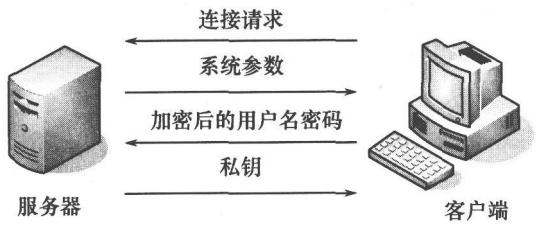

图 9.6 客户端和服务器端安全通信示意图

用户在本地计算机向服务器发送请求,以便获得当前系统参数,之后用户将经过加密处理的用户名和密码发送给服务器,登陆服务器。服务器检查用户的用户名和密码,如果通过,则用户登陆成功,将用户的私钥发送给用户,用户解密存放在本地客户端上的 AES 密钥,并约束用户的访问控制权限;否则,用户登陆不成功,需要重新登陆。

(2) 登陆和退出

登录成功后,用从服务器得到的私钥,解开存放在本地数据库的 AES 对称密钥,可以对文件进行解密、修改。退出后,通过密钥定时更换机制,用户通过从服务器得到的新私钥对存放在本地数据库的 AES 对称密钥进行加密。如图 9.7 所示。

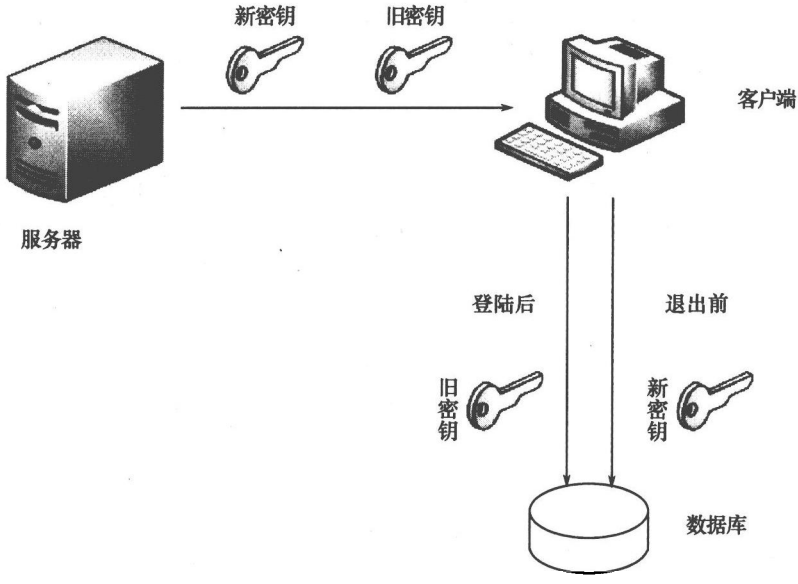

图 9.7　用户登录和退出

(3) 对本地文件进行安全保护

解密时,从已打开的数据库中读取密钥,对已加密的文件解密,将解密后的文件存入临时文件夹中。加密时,产生一个随机的原始密钥,对文件进行对称加密,完成加密后将原文件删除,并将产生的该原始密钥存入本地的数据库。如图 9.8 所示。

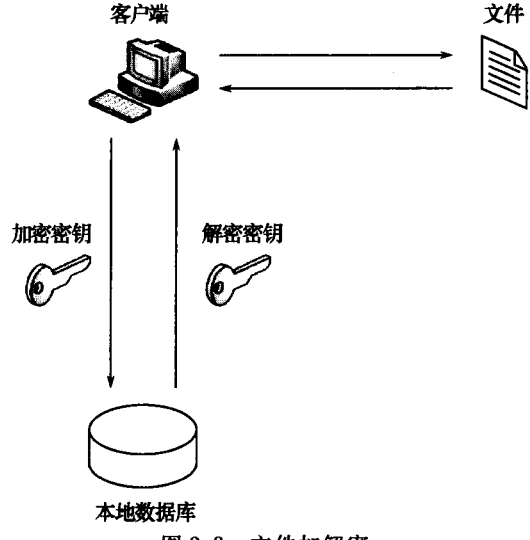

图 9.8　文件加解密

.重要名词术语中英文对照

ABDHE 问题	ABDHE, augmented bilinear Diffie-Hellman exponent problem
ABDHI 问题	ABDHI, augmented bilinear Diffie-Hellman inversion problem
BDHI 问题	BDHI, bilinear Diffie-Hellman inversion problem
BDH 问题	BDH, bilinear Diffie-Hellman problem
CDH 问题	CDH, computational Diffie-Hellman problem
DBDHI 问题	DBDHI, decision bilinear Diffie-Hellman inversion problem
DHI 问题	Diffie-Hellman inversion problem
DH 算法	Diffie-Hellman algorithm
DH 问题	Diffie-Hellman problem
GBDH 问题	GBDH, gap bilinear Diffie-Hellman problem
LBDH 问题	LBDH, list bilinear Diffie-Hellman problem
RSA 算法	RSA, Rivest Shamir Adleman algorithm
SDHI 问题	SDHI, strong Diffie-Hellman inversion problem
wBDHI 问题	weak bilinear Diffie-Hellman inversion problem
安全多方计算	secure multi-party computation
安全性分析	security analysis
标准签名	SS, standard signature
标准身份鉴别	SI, standard identification
不经意传输	oblivious transfer
不可区分性	indistinguishability
部分私钥提取算法	part of the private key extraction algorithm
单向函数	one-way function
敌手	adversary
第三方权利受约束的 IBE 方案	A-IBE, accountable authority identity-based encryption scheme
动态广播加密	DBE, dynamic broadcast encryption

对称加密算法	symmetric cryptographic algorithm
多接收者密钥封装机制	mKEM, multi-receiver key encapsulation mechanism
非退化性	non-degeneracy
分层的基于身份广播加密	HIBBE, hierarchical identity-based broadcast encryption
分层的基于身份加密	HIBE, hierarchical identity-based encryption
概率性算法	probabilistic algorithm
根密钥	root key
公共密钥体制	PKG, public key cryptosystem
公开参数	public parameters
公开矩阵	public matrix
公钥	public key
公钥基础设施	PKI, public key infrastructure
公钥密码算法	public key cryptography algorithm
公钥替换	public key replacement
公钥证书	public key certification
固定长度	constant size
广播加密	BE, broadcast encryption
国际数据加密算法	IEDA, international data encryption algorithm
机密性	confidentiality
基于身份的广播加密	IBBE, identity-based broadcast encryption
基于身份的加密	IBE, identity-based encryption
基于身份的密码体制	IBC, identity-based crytosystem
基于身份的密码学	IBBC, identity-based cryptography
基于身份的签名	IBS, identity-based signature
加密	encryption
截断判定性 q-ABDHE 问题	q-ABDHE, truncated decision q-augmented bilinear Diffie-Hellman exponent problem
解密	decryption
解密询问	decryption query
静态安全	static state security
抗冲突杂凑函数	collision-resistant hash function
可计算性	calculability

可信计算密码支撑平台	cryptographic support platform for trusted computing
可证明安全	provable security
空间复杂性	space complexity
零知识证明	zero-knowledge proof
秘密密钥	secret key
秘密值	secret value
密码 Hash 函数	cryptographic Hash function
密码体制	cryptosystem
密码校验函数	cryptographic check function
密码学	cryptology
密文	ciphertext
密文空间	ciphertext space
密钥	key
密钥分发	key distribution
密钥分发中心	key distribution center
密钥管理	key management
密钥交换	key exchange
密钥生成中心	KGC, key generate center
密钥替代攻击	key replacement attack
密钥托管	key escrow
密钥协商	key agreement
明文	plaintext
明文空间	plaintext space
模糊的基于身份加密	FIBE, fuzzy identity-based encryption
判定的 DH 问题	DDH, decisional Diffie-Hellman problem
人工终止	artificial abort
认证算法	authentication algorithm
认证中心	CA, certification authority
身份鉴别	identity authentication
生日攻击	birthday attack
时间复杂性	time complexity
输出反馈工作模式	OFB, output feedback operation mode
数字签名	digital signature
双线性映射	bilinear map

私钥	private key
私钥查询	private key query
私钥生成器	private key generator
私钥提取	private key extraction
随机多项式	*random polynomial*
随机数	random number
随机预言模型	random oracle model
挑战者	challenger
椭圆曲线	elliptic curve
椭圆曲线密码算法	ECC, elliptic curve cryptography algorithm
伪随机数	pseudorandom number
伪随机序列生成器	pseudorandom sequence generator
伪造签名	forged signature
无证书公钥密码方案	CL-PKE, certificateless public key encryption scheme
无证书公钥密码体制	CL-PKC, certificateless public key cryptosystem
无证书签名	certificateless signature
线性反馈移位寄存器	linear feedback shift register
线性密码分析	linear crypt analysis
消息认证码	MAC, message authentication code
选择密文安全	chosen-ciphertext security
选择明文安全	chosen-plaintext security
循环乘法群	cyclic multiplicative group
循环加法群	cyclic additive group
一次性密钥	one-time key
一次性签名	*one-time signature*
有限域	finite field
阈值	threshold value
证书撤销	certificate revocation
主密钥	master key